Kundinriktad multifaktorautentisering inom bilindustrin

Kandidatarbete för Data- och Informationsteknik

Johan Blom
Sam Sohrabpour

Institutionen för Data- och Informationsteknik
CHALMERS TEKNISKA HÖGSKOLA
GÖTEBORGS UNIVERSITET
Göteborg, Sverige 2020

Examensarbete 2020

Johan Blom

Sam Sohrabpour

CHALMERS
UNIVERSITY OF TECHNOLOGY

Institutionen för Data- och Informationsteknik
Chalmers Tekniska Högskola
Göteborgs Universitet
Göteborg, Sverige 2020

Kundinriktad multifaktorautentisering inom bilindustrin
Johan Blom
Sam Sohrabpour

Handledare: Sakib Sistek
Examinator: Jonas Duregård

Kandidatarbete 2020
Institutionen för Data och Informationsteknik
Chalmers Tekniska Högskola
SE-412 96 Göteborg
Telefon: 031-772 1000

The Author grants to Chalmers University of Technology and University of Gothenburg the non-exclusive right to publish the Work electronically and in a non-commercial purpose make it accessible on the Internet.

The Author warrants that he/she is the author to the Work, and warrants that the Work does not contain text, pictures or other material that violates copyright law.

The Author shall, when transferring the rights of the Work to a third party (for example a publisher or a company), acknowledge the third party about this agreement. If the Author has signed a copyright agreement with a third party regarding the Work, the Author warrants hereby that he/she has obtained any necessary permission from this third party to let Chalmers University of Technology and University of Gothenburg store the Work electronically and make it accessible on the Internet.

Institutionen för Data- och Informationsteknik Göteborg 2020

Abstract

In our increasingly digitized world every meaningful action starts with a simple question: are you really you? The objective of this report was set out to explore, recommend and implement a customer focused step-up authentication process aimed primarily at the auto industry. A mobile application was developed to test the added authentication steps required for the end user. The project was limited to user scenarios within the mobility sector but the recommended process can easily be applied to other industries. The report examines how a customer facing step-up verification can be accomplished with Multi Factor Authentication and types of factors that were both secure and frictionless from a user experience perspective. The project was achieved with the help of the agile framework Scrum with visual studio as the environment for application development. The report also discusses alternative methods that could be used instead to improve a secure user experience as well as what a future with Multi Factor Authentication might look like.

Sammandrag

I vår alltmer digitaliserade värld börjar varje meningsfull handling med en enkel fråga: är du verkligen du? Syftet med denna rapport var att undersöka, rekommendera och genomföra en kundfokuserad autentiseringsprocess riktad främst inom bilindustrin. En mobilapplikation utvecklades för att testa de autentiseringssteg som krävs av slutanvändaren. Projektet var begränsat till användarscenarier inom personbilssektorn men den rekommenderade processen kan enkelt tillämpas inom andra branscher. Rapporten undersöker hur en kundinriktad verifiering kan genomföras med stöd av multifaktorautentisering och de typer av faktorer som anses både säkra och användarvänliga ur ett slutanvändarperspektiv. Projektet genomfördes med hjälp av det agila ramverket Scrum med verktyget visual studio som miljö för applikationsutvecklingen. Rapporten lyfter även alternativa metoder som kan användas för att förbättra en säker användarupplevelse och hur en framtid med multifaktorautentisering kan se ut.

Nyckelord: Multifaktorautentisering (MFA), Applikation, kundflöde, biometri

Förord

Vi vill tacka Alexander Crayvenn och Sakib Sistek för deras engagemang och hjälp vilket gjort detta arbete möjligt och intressant.

Terminologi och förkortningar

2FA: Två-faktor autentisering
IOT: Internet of Things
iOS: iPhone Operating System
MFA: Multi-factor autentisering
PIN: personal identification numbers
SSO: Single Sign-On
OTP: One-Time Password
USB: Universal Serial Bus
ADB: Android Debug Bridge

Innehåll

1 Introduktion

1.1 Bakgrund

I vår uppkopplade värld börjar varje betydelsefull handling med en enkel fråga: Är du verkligen du? Den digitala transformationen har förändrat kunders sätt att interagera med och konsumera tjänster, och ens digitala identitet förblir kärnan i varje steg av kundresan. Att kunna skapa och erbjuda personifierade tjänster ses numera som en hörnsten inom många industrier, just för att kunna stärka kundrelationer i de steg kunden genomgår med ett varumärke och på så sätt även behålla kundlojaliteten. Detta gäller numera även för biltillverkare som historiskt inte haft lika stor fokus på direkta kundrelationer så som aktörer inom t.ex: e-handeln.

Med bilindustrins stora kliv mot att erbjuda digitaliserad synergi mellan bil, kund och tjänster denne efterfrågar, behöver biltillverkarna balansera behovsbilden för bekväm åtkomst till tjänster med reducerad risk för obehörigt tillträde.

1.2 Syfte

Under många år har vi valt att skydda våra tillgångar med lösenord som med tiden blivit allt mer komplexa. Men lösenord är inte alltid en tillräcklig säkerhetsfaktor eftersom 81 procent av hacking attacker är kopplade till lösenord[14]. Tekniker för dataintrång har också utvecklats med tiden, och rapporterade överträdelser pekar mot utnyttjandet av stulna eller svaga lösenord[15]. Trots dess ökade komplexitet senaste 20 åren förblir våra lösenord en viktig del av hur vi skyddar vår data och får åtkomst till tjänster som t.ex. styr våra uppkopplade hem och bilar. Men själva lösenordet, som en vanligt förekommande säkerhetsmekanism, är inte tillräcklig för att verifiera identiteten av resursägaren (kunden). Hur kan då bilföretagen gå över till en säkrare metod för autentisering utan att försämra användarupplevelsen?

1.3 Mål

Detta arbete kommer:

- undersöka och rekommendera en autentiseringsmetod där användaren behöver utföra ytterligare autentiseringshandlingar efter behov och kravbild.

- föreslå riktlinjer för tillämpning av en autentiseringsmetod baserat på användarfall som identifierats inom bilindustrin och dess riktning inom mobilitetslösningar.

- tillämpa en autentiseringsmetod med fokus på både säkerhet och användarvänlighet.

1.4 Avgränsningar

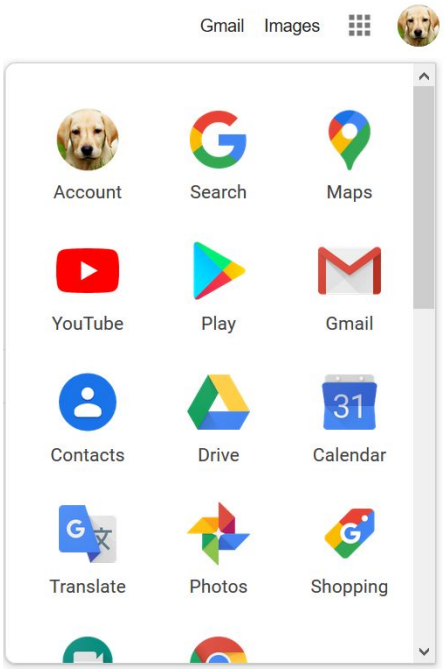
- Applikationen som utvecklades i detta arbete kopplas inte mot en fysisk bil och dess tjänster.
- Funktionaliteten som togs fram i applikationen är oberoende av bilmärke. Då gruppen hade tillgång till Volvos mobila applikation nyttjades denna som en statisk design-komponent och därmed övervägdes inte design från andra bilmärken.
- Implementering för iOS valdes bort då man inte hade tillgång till rätt hårdvara vilket försvårade test och verifikation av mobilapplikationen.
- Att införa en dynamisk autentiseringsmetod baserat på ens position hade lyft andra säkerhetsaspekter, men funktionaliteten blev bortprioriterad då denna är avhängande av tredje part leverantörer.

2 Teori

2.1 Single Sign On

Single Sign-On (SSO) är en metod som tillåter användare att logga in på flera olika applikationer med ett och samma konto. Implementeras Single Sign-On på rätt sätt så förbättras både effektiviteten och användarupplevelsen av registreringen då man inte längre behöver komma ihåg ett extra användarnamn och lösenord för att logga in. För att detta ska fungera så måste det finnas ett förtroende mellan applikationerna. På grund av detta förtroende litar applikationerna på att användaren är autentiserad på ett säkert sätt vid första inloggningen och därmed behöver användaren inte logga in igen för att få tillgång till dem.

Single Sign-On kan tros vara något som man inte ser dagligen men har man exempelvis ett google konto så använder man sig redan av Single Sign-On. Så fort du loggar in på ditt google konto så loggas man även in på sin Gmail, Drive, youtube och google play konton som man kan se i den nedanstående bilden (**Figur 1**).



Figur 1 är en skärmdump som visar alla applikationer som man nu kan använda med google kontot som man har loggat in med. Detta är utfört med hjälp av Single Sign-On (SSO).

2.2 Två-faktor autentisering

Två-faktor autentisering (2FA) är en tvåstegs autentiseringsprocess som har för avsikt att tillhandahålla en extra nivå av säkerhet[1] . Den extra säkerheten uppnås genom att användaren måste autentisera sig själv genom ett extra steg istället för att bara autentisera sig med ett vanligt lösenord. Alla extra steg är inte identiska utan kan variera, stegen har olika nivåer av säkerhet, men alla är säkrare än inloggning med bara ett lösenord.

OTP (One-Time Password) är ett exempel på ett extra steg vid inloggning, det fungerar genom att vid varje inloggning efter man skrivit sitt användarnamn och lösenord så ska man skriva in en kod som bara håller i en angiven tid, vanligtvis inte längre än 30 sekunder. Denna kod är unik för varje inloggning och visas i en extern app man kan installera på telefonen eller datorn. Utan 2FA så räcker det för en hackare att få åtkomst till ens lösenord för att kunna logga in, med 2FA försvåras detta.

2.3 Multifaktorautentisering

Multifaktor autentisering (MFA) är precis som 2FA en process för att autentisera sig på ett säkrare sätt än att bara använda ett lösenord. MFA består av två eller flera säkerhetssteg man måste använda för att verifiera sig, till skillnad från 2FA som inte har mer än två, därav namnet multi-faktor. Man kan till exempel identifiera sig själv genom vem man är (via tumavtryck) eller genom vad man har (en fysisk nyckel), vilket man även kan använda med 2FA.

En positiv egenskap med MFA är att det kan vara anpassningsbart med vilket eller hur många säkerhetssteg som användaren behöver verifiera. En användare som befinner sig i ett land som personen vanligtvis inte befinner sig i eller som kan klassas som mindre säkert, kan tvingas verifiera fler och komplexare säkerhetssteg. Ett exempel på detta är om en person vanligtvis är bosatt i Sverige och vill logga in från Marocko så måste personen identifiera sig som vanligt, plus en eller fler verifieringar som till exempel visa fingeravtryck för att konstatera man verkligen är rätt användare.

Fördelen med MFA gentemot 2FA är att det kan vara mer former av autentisering jämfört med bara två i 2FA, ju mer verifieringar användaren behöver göra desto säkrare är det. Speciellt om man använder fingeravtryck som autentisering, vilket är svårt för en potentiell hackare att få tag på. Men fördelen kan även vara en nackdel om man använder det fel, eftersom ju fler säkerhetssteg man har desto bättre är det

för säkerheten, men en annan viktig punkt när det gäller autentisering är användarupplevelsen. En användare vill kunna logga in eller autentisera sig snabbt och kunna utnyttja sitt konto direkt och inte behöva verifiera sig flera gånger, vilket tar mer tid ju fler steg man har. Därför måste man göra en avvägning av hur mycket en användare behöver identifiera sig utan att försämra upplevelsen för den, eftersom med alla alternativ en kund har idag så blir man lätt kräsen och använder en annan app om man inte gillar hur appen upplevs.

2.3.1 Typer av autentisering

Det finns olika typer av autentisering man kan använda sig av vid verifiering av individer med MFA, några säkrare än andra. Dessa typer kommer generellt i tre former:

- Något man vet: Det vill säga något man måste komma ihåg och sedan visa eller utföra för att verifiera sig, exempelvis vanliga lösenord och kodord.
- Något man är: Med detta menas delar av kroppen som kan användas som en typ av verifiering som till exempel inläsning av fingeravtryck, avläsning av ansiktet och röstigenkänning. Denna typ av verifiering kallas för biometrisk autentisering.
- Något man har: Detta är fysiska objekt som man kan använda för att verifiera sig, såsom bilnycklar, smarttelefon och token enheter till exempel.

Det är med dessa typer man kan kombinera två eller fler för att skapa en applikation med multifaktor autentisering och man vill ha det så säkert som möjligt medans det är enkelt att använda för kunden.

Autentisering med något man vet såsom lösenord är den minst säkraste typen eftersom användningen av lösenord som verifiering tvingar användare att tänka ut och komma ihåg avancerade kombinationer av siffror, bokstäver med mera för att få ett så säkert lösenord som möjligt. Användare rekommenderas också att ha unika lösenord för varje konto för att reducera risken att bli hackad. Användare måste hantera allt från 25 till 85 lösenord[1] idag och med digitaliseringen av samhället kommer denna summa växa. Vid hantering av så många lösenord kan användaren lätt bli lat och återanvända lösenord, vilket betyder att om ett konto blir hackat så får hackaren även åtkomst till de andra kontona som delar samma lösenord.

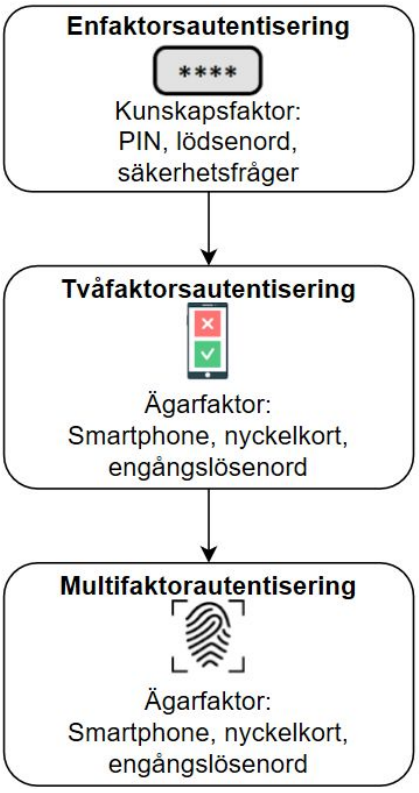
Med autentisering genom något man har som till exempel en bilnyckel är det svårare för en hackare att göra dataintrång, eftersom det krävs en fysisk nyckel. Men användaren måste hålla koll på den och bevara den på ett säkert ställe, samt bära omkring på den vid verifieringen, att ha en fysisk nyckel för alla ens konton kan lätt

bli frustrerande för en användare och är därmed inte den bästa lösningen. Det kostar även pengar att tillverka det fysiska objektet och kan tappas bort.

För att stärka säkerheten kan man lägga till biometrisk autentisering, utöver de andra typerna för att skydda från dataintrång. Med biometrisk autentisering så behöver man inte komma ihåg något som till exempel ett lösenord utan man kan autentisera sig med något man alltid har med sig, som med ett fingeravtryck eller ansiktsigenkänning, vilket är vanliga metoder av biometrisk autentisering. Biometrisk autentisering är skyddad mot de flesta typer av cyberattacker[2] och är samtidigt mer bekväm för användaren än vanliga lösenord att använda enligt en undersökning[3], vilket gör detta till en lämplig typ av autentisering med MFA.

Autentisering med sitt ansikte är en säkrare metod på iOS än Android eftersom Apple har lagt ner mycket teknologi på det med teknik som en 3D karta av ens ansikte[16]. Androids version av ansiktsläsning är inte av samma säkerhet då test har visat att vissa av deras telefoner kan autentiseras med fotografi av någons ansikte[17]. Till följd av skillnaden av säkerhet så måste man ha det i åtanke om båda metoderna ska finnas tillgängliga.

Figur 2 som summerar utvecklingen av autentiseringsmetoder:



Figur 2. Evolutionen av autentiseringsmetoder från en faktors autentisering till multifaktorautentisering.

3 MFA i användarcentrerad utveckling

3.1 Användarfall

Multifaktorautentisering har många potentiella användningsområden inom bilindustrin och personifierade mobilitetslösningar för att förbättra säkerheten men samtidigt inte försämra kundupplevelsen. Användarfallen som listas nedan är bara några exempel på områden där MFA kan implementeras.

3.1.1 Den digitala bilnyckeln

Snart är den klassiska bilnyckeln som en fysisk ikon och del av bilen historia. Ett annat vanligt alternativ det senaste åren för åtkomst till bil har varit genom knapptryckning på en bilnyckel som mest efterliknar en minnessticka eller en plastbit i form av ett kreditkort.

En kommande standard som ska underlätta våra liv är den digitala bilnyckeln[5]. Den digitala nyckeln kan vara i en smart enhet som en mobiltelefon där man kan ha en applikation som har översikt över ens bils tillstånd. Med en digital nyckel kan man få rätt åtkomst till bilen utan knapptryckning eller liknande[6], förutsatt att man har sin smarta enhet till hands så att bilen kan känna av den och veta att du är du. Men hur ska bilen verkligen veta att du är du, det är där MFA kommer in och kan användas för att säkra autentiseringen.

För att kunna använda nyckeln måste man kunna autentisera sig och sätta upp nyckeln så att bilen senare vet vem man är, detta kan göras med hjälp av MFA, alltså flera olika steg på ett säkert sätt. Om man ingår i en bilpool eller önskar att familj och vänner också kan få tillgång till fordonet kan man göra det med digital delning av nyckeln. Även här kan MFA användas så inte obehöriga får åtkomst.

3.1.2 Tillgång till bil

Det finns olika nivåer av tillgång till en bil. Med den digitala nyckeln kan man bestämma vilken behörighet en person ska ha till ett fordon. Vill man att personen bara ska kunna öppna bagageluckan och inte kunna starta bilen så kan ägaren välja det i inställningarna. Detta är användbart till exempel om man vill ha något levererat till sin bil men inte kan närvara fysiskt, då kan man ge varubudet tillgång till endast bagageluckan, som sen lägger varan i bilen. Allt detta går att göra i sin smarta enhet och med hjälp av MFA kan man autentisera individerna som ska ta del av fordonet[4].

3.1.3 GDPR förfrågningar

Efter att EU:s allmänna dataskyddsförordning (GDPR) trätt i kraft för ett utökat skydd av personuppgifter har företag behövt forma nya säkerhetsprocesser i relation till hur personuppgifter kan behandlas och hur man säkerställer rätt åtkomst till dessa. Syftet med GDPR är att skydda individens rättigheter i relation till behandlingen av deras personuppgifter.

Företag som behandlar personuppgifter och som antingen (i) är etablerade inom EU eller (ii) erbjuder varor eller tjänster till personer inom EU eller övervakar beteendet hos sådana personer omfattas av den nya dataskyddsförordningen.

I och med individens rättigheter i relation till behandlingen av personuppgifter och de skyldigheter att informera individen om den rättsliga grunden samt förse denne med uppgifterna vid begäran har satt nya interna krav på säker hantering och delning av persondata.

En robust MFA lösning för kundidentitet och åtkomsthantering kan hjälpa till att lösa många av de tekniska kraven för att underlätta hantering av kundfall riktade mot dennes rättighet att komma åt ens data som företaget behandlar. MFA kan hjälpa verifiera kundernas behörighet genom att be användaren uppge ytterligare bevis på sin identitet.

3.1.4 Ändring av personkonto-inställningar

Vid ägande av ett konto där ens uppgifter kan vara känsliga eller essentiella för att användandet av kontot ska fungera som det ska, som exempelvis att ändra bilinställningar eller ens lösenord,så vill man ha stark säkerhet. Det är viktigt att rätt person ändrar inställningar så inte en obehörig kan ändra inloggningsuppgifter och därmed låsa ut en från sitt egna konto.

För att autentisera rätt person så kan MFA användas för att få extra säkerhetssteg och minska risken att få sitt konto stulet. Exempelvis kan användaren behöva autentisera sig om den vill ändra lösenord eftersom det är viktig del av säkerheten, men inte vid byte av användarnamn därför att det är inte samma säkerhetsrisk angående det och därmed bara har extra verifiering då det behövs.

3.2 Användarupplevelse av autentisering via flera faktorer

Vid användning av flera faktorer så är det viktigt att välja faktorer som både är säkra men också något som inte användaren tycker är besvärligt. Eftersom många användare är vana med bara lösenord som autentisering kan det lätt bli frustrerande om denna individ måste verifiera sig flera gånger, därmed måste faktorerna implementeras rätt men först är det bra att ta undersöka vad användare tycker om fler faktorer.

I en undersökning[9] så visar det sig att 54 procent av de tillfrågade använder mer än en faktor vid autentisering frivilligt, varav kod via sms är den vanligaste typen, detta betyder att många redan är vana med flera faktorer och underlättar därmed användning av MFA. Problemet med just kod via sms är att det inte stoppar en person som har stulit ens telefon, eftersom koden kommer till just telefonen och därmed skulle ge förövaren åtkomst till ens konto, till följd därav inte det bästa för säkerheten.

I undersökningen så visar det sig även att 45 procent använder fler faktorer när tjänsten de använder erbjuder det, vilket är positivt för användning av MFA. Det man får ha i åtanke är att dessa siffror behöver inte stämma för allmänheten eftersom i denna undersökning så var majoriteten mer förmögna än genomsnittet och därmed inte representativ för hela befolkningen.

I en annan studie som undersökt flera undersökningar kring MFA[10] så är slutsatsen att MFA förbättrar säkerheten genom implementering av flera steg men även visar att användbarheten är en utmaning och kan förbättras. Studien visar även att många undersökningar kring användbarheten ofta studerar unga vilket kan leda till en falsk uppfattning eftersom unga hanterar tekniken annorlunda. För att förbättra användningen av MFA så bör undersökningarna inkludera en mer mångfaldig testgrupp.

3.3 Utmaningar med MFA förvaltning

Med MFA så finns det även utmaningar man måste ha i åtanke vid införande av det i ens applikation så att alla ska kunna ha möjligheten att autentisera sig.

- Användbarhet - Det måste vara lätt och får inte ta för långt tid för användaren att verifiera sig. Användarens preferenser för val av autentiseringstyp kan också variera och är därför bra att erbjuda flera alternativ så användaren kan

använda sin prefererade metod. Det ska passa för alla åldrar, äldre kanske föredrar en annan metod av verifiering gentemot yngre, eftersom det visar sig att den yngre generationen spenderar 50% mindre tid på att autentisera sig[8].

- Integration - MFA är beroende av hårdvaran och måste därmed kunna integrera med ny och gammal hårdvara så det fungerar som det tänkt. Vissa enheter som till exempel Apples iphone X har inte tillgång till fingeravtryckskläsning men har tillgång till avläsning av ansiktet, därmed är det bra att ha ett flexibelt system så att båda alternativen är tillgängliga för användaren så att den kan välja det ens enhet har möjlighet till. Det finns även enheter som inte har tillgång till någon av de biometriska metoderna, då kan en lösning på det vara att användaren skriver in en PIN-kod eller använda One-Time Password istället, vilket dock gör att säkerheten kan försämras.
- Säkerhet - Även om säkerheten förbättras med MFA så är det inte felsäkert, i samband med att tekniken för säkerheten utvecklas så utvecklas även attackerna mot den, vilket gör att man konstant måste hitta förbättringar för att ha en trygg säkerhet. På grund av beroendet MFA har av hårdvaran det är tillämpat i så kan det uppstå säkerhetsrisker om hårdvaran inte är tillräckligt säkerhets utrustad som det borde vara. Detta kan leda till en lyckad attack för potentiella hackare även om autentisering typerna teoretiskt ska kunna stoppa just den sortens attack men inte kan på grund av felaktig hårdvara.
- Känslighet - Det man får tänka på med det olika typerna av autentisering är att det fungerar i en optimal testning miljö, men det kanske inte fungerar i sämre förhållanden. Med röstigenkänning som verifieringstyp kan det vara problematiskt att få enheten att höra en i högljudda områden som till exempel nära trafikerade vägar och därmed måste lämpliga alternativ erbjudas.

Möjligheterna med flexibel MFA om man har dessa utmaningar i åtanke är många. Ett scenario på hur flexibel MFA kan användas är att användaren har ett lösenord eller PIN för att verifiera sig, samt utöver det behöver visa någon form av biometrisk autentisering såsom fingeravtryckskläsning. Om det misslyckas eller inte finns tillgängligt så kan man behöva använda sig av en annan kombination av faktorer vilket användaren blir uppmanad att visa.

Med detta system så kan man studera hur användaren beter sig vid autentiseringen och hur den interagerar med enheten, därmed kan man förbättra momentet för användaren ju mer den interagerar med enheten, vilket på sikt ger en bättre användarupplevelse.

4 Metod

I detta kapitel beskrivs det hur arbetet har utförts och vilka verktyg som användes för att utföra det. Med metoderna medföljer även en förklaring varför de valdes.

4.1 Verktyg

I projektet så användes diverse metoder för att få en så effektiv arbetsprocess som möjligt och nå ett önskat resultat.

- Github valdes eftersom det är ett simpelt sätt att dela kod med sin kollega på över internet. Man kan både dela med sig det man själv gjort, men även hämta det sin kollega gjort för att kunna använda det.
- Visual Studio valdes som utvecklingsmiljö i kombination med pluginet Xamarin som möjliggör utveckling av mobila appar som både kan köras igång med Android och Iphone smartphones. Utvecklingsmiljön användes för att kunna skapa en replika applikation av Volvos on call app och för att införa fingeravtrycksläsning som säkerhetsautentisering i appen.
  - Tillägg på Visual studio Xamarin som LiveXaml möjliggjorde designändringar på mobilappen i realtid och “Android debug bridge” för att kunna köra igång mobilappen på mobilen trådlöst över nätet.
  - Packet tillägg som möjliggör fingeravtrycksläsning och databas användning.
- Design verktyget Figma användes för att kunna demontera och förstå “Volvo on call” designen så att man efteråt kunde replikera och bygga vidare på temat.
- Det agila ramverket scrum används för projektarbetet så att projektmedlemmarna i gruppen kan maximera effektiviteten, förståelsen bakom andras kunskaper i gruppen och så att gruppen kan anpassa sig till nya miljöer på ett smidigt sätt.
- Volvo’s design på fonter och bakgrund användes med anledning av Sigmas samarbete med Volvo.
- Android Debug Bridge användes för att möjliggöra en trådlös USB uppkoppling över nätet.
- Hot Reload användes vilket möjliggjorde direkt kompilering i realtid så att mobilapplikationen uppdateras så fort någon ny kodfil sparades till skillnad från innan då projektmedlemmarna var tvungna att starta om hela applikationen för att testa den nya koden igen.

4.2 Arbetsmetod

4.2.1 Val av arbetsmetod

Arbetet har utförts med hjälp av den agila arbetsmetoden scrum, vilket är ett ramverk för hur man arbetar inom lag för systemutveckling på ett iterativt sätt, därav agilt.

Scrum går ut på att man arbetar i korta cykler som kallas sprinter och i varje sprint ska man ha en ny färdig funktionalitet som ger värde på ens produkt så man har något att visa för intressenter. Längden på en sprint kan variera men i detta arbete så var längden två och en halv vecka, kort nog för att regelbundet undersöka utvecklingen men samtidigt långt nog för att skapa något av värde.

I slutet av varje sprint visas det man har gjort för intressenter så dessa kan dela sina synpunkter vilket man har i åtanke vid arbetet nästa sprint. Fördelen med scrum är förmågan att kunna hantera förändringar genom att konstant få synpunkter från kunder och intressenter så arbetet kan förbättras ständigt.

En annan stor fördel är riskminimering, ifall man påbörjat en funktion till produkten och sen vid redovisningen har intressenten ändrat sig när den ser implementationen och vill ha något annat istället. Då kan man avbryta arbetet på funktionen och därmed spara tid och resurser. Om man istället hade fått veta långt senare att funktionen var onödig hade resurser gått till spillo, så det är inte lika stor risk att implementera nya funktioner eftersom till följd av regelbunden inspektion så kan fel rättas snabbare än med vattenfallsmetoden till exempel.

En nackdel med scrum är att på grund av att man arbetar i sprintar och inte planerar projektet fullt i detalj från början, så kan det vara en viss osäkerhet angående hur slutprodukten ska vara vilket kan vara ansträngande för dem involverade.

Ett annat alternativ till scrum som kunde användas var vattenfallsmetoden vilket är en sekventiell systemutvecklingsprocess gentemot scrums iterativa process. I vattenfallsmetoden så finns det olika faser: förberedelse, etablering, analys, design, konstruktion, test, produktionssättning och underhåll. Faserna fungerar som ett flöde nedåt, därav namnet vattenfall, där faserna uppfylls i ordning.

Fördelen med denna metod är det är strukturerat och man upptäcker problem tidigt i projektet eftersom man planerar hela projektet i detalj innan man påbörjar arbetet. Detta är fördelaktigt när man ska bygga hus till exempel, huset byggs från en färdig ritning och teknikerna för att bygga huset ändras normal inte drastiskt mitt under byggandet. Men om teknikerna och arbetsmarknaden utvecklas konstant så att

projektets grundvision blir föråldrat och meningslöst så hänger inte vattenfallsmetoden med. Detta är ett stort problem vid systemutveckling inom IT eftersom den marknaden utvecklas konstant och därmed måste kunna hantera förändringar i projektet, så att planen man hade förra månaden kan ändras till en mer passande och vinstgivande.

Scrum valdes som arbetsmetod på grund av dess agila arbetssätt vilket är fördelaktigt vid systemutveckling inom IT och att kunna hantera förändringar på ett enkelt sätt, samt få regelbundna synpunkter från handledare och företagsrepresentanter.

4.2.2 Planering

Det första två veckorna bestod av planering av arbetets upplägg och vilka applikationens huvudfunktioner skulle vara, samt planering av vilken utvecklingsmiljö som passade bäst för arbetet. Planeringen utfördes genom läsning av åtskilliga artiklar angående autentisering för att fördjupa sig kring ämnet och ta reda på varför man ska välja just multifaktor autentisering.

Artiklar om vilka autentiserings typer som var smidigast för användaren studerades för att ta reda på vilka man ska välja. I samband med diskussioner med företagsrepresentant så togs ett slutmål för applikationen fram med dess önskade funktioner. Utvecklingsmiljön för arbetet valdes, vilket blev Visual Studio Xamarin på grund av dess möjlighet att hantera både IOS och Android.

4.3.1 UX-design rekommendationer

Multifaktor autentisering i sig är en funktion som förbättrar användarupplevelsen för användarna eftersom att man snabbt och smidigt kan få tillgång till sitt konto med ett fingeravtryck eller ansiktsläsning istället för exempelvis logga in manuellt.

För att kunna optimera användarvänligheten (Usability) så krävs det att designen är smidig och lätt att förstå. Några exempel på detta finns i MFA sidan (**Figur 8**) där man kan se all information som behövs för att komma vidare utan att behöva scrolla eller att gå till en annan sida (**visibility**)[11].

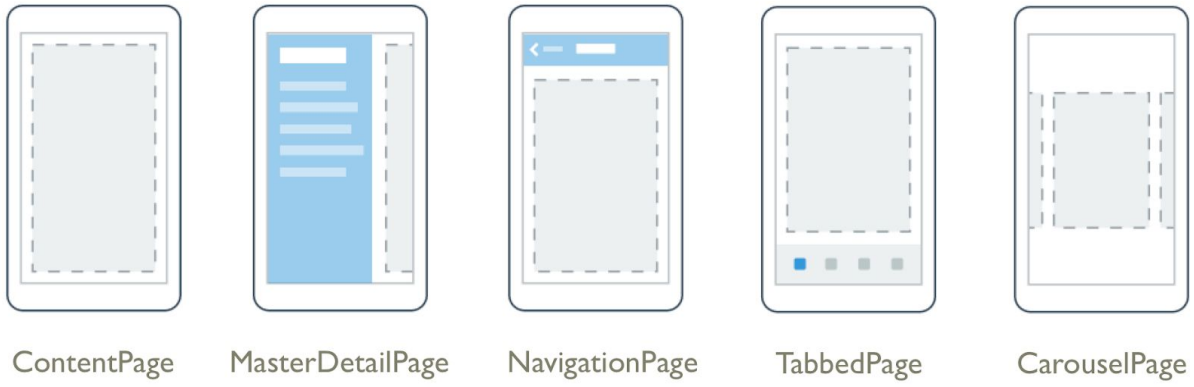
Utöver detta så har vi andra stödjande metoder för användarvänligheten som bland annat **affordance** som innebär att man kombinerar knapparna med ikoner som många redan känner igen från andra källor så att de direkt kan förstå vad knapparna gör utan förklaring.

Utöver detta så finns även alternativet att välja konto som man har sparat så att man slipper behöva logga in igen då man behöver byta konto, detta medför alltså en ökning av **utilities** vilket därmed också förbättrar användarvänligheten[12].

När det kommer till användarupplevelsen så är användarvänligheten en faktor som påverkar den, men användarupplevelsen handlar också om känslorna som användarna får när de ser på produkten. Därför så är det viktigt att vara konsistent med teman då ny design skapas. Exempel på detta i MFA sidan (**Figur 8**) är ljusgråa bakgrundsfärgen, svarta textfärgen och Sans-Serif text typsnittet som alltid används i applikationens design.

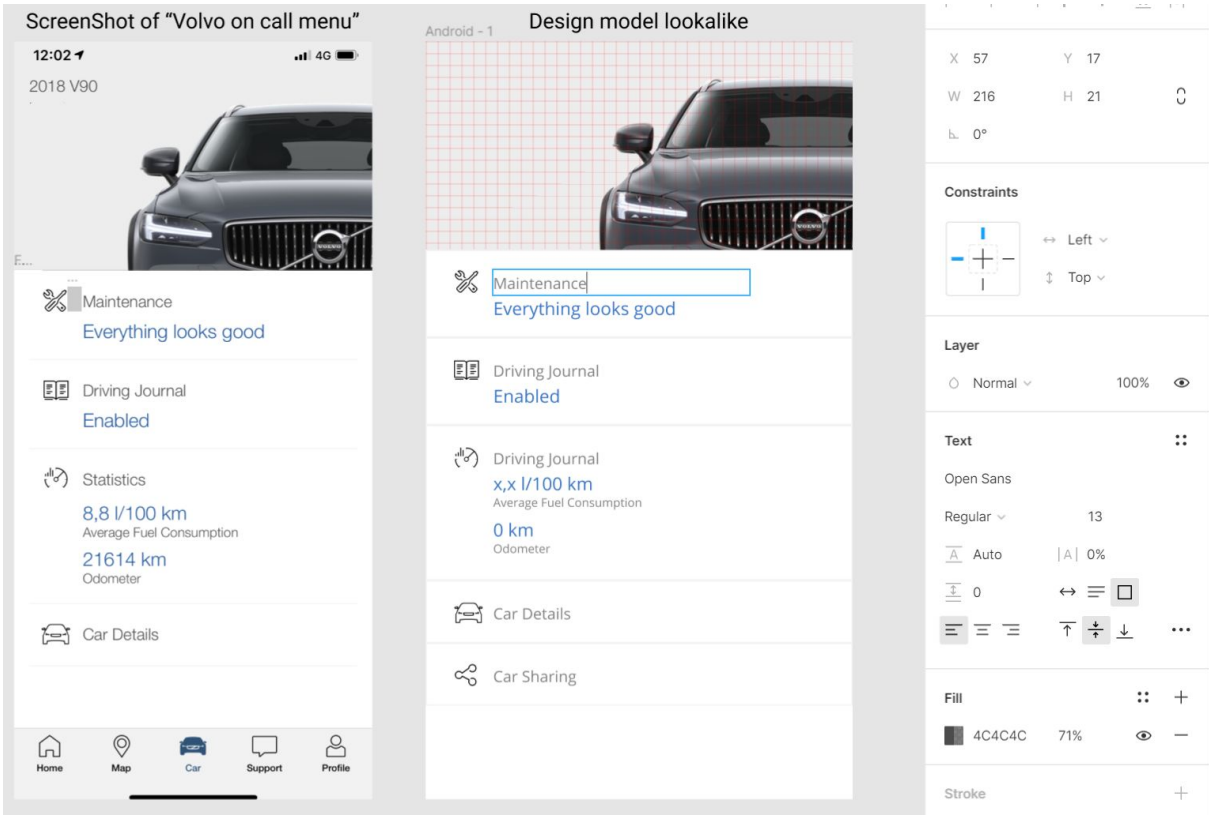
När det kommer till design av applikationer med Visual Studio Xamarin så har man fem olika typer av sidor (som man kan se på **Figur 3**).

Vi har Content Page som är en tom sida, MasterDetailPage som har en knapp som får en större meny att fällas ut, NavigationPage som där man flyttar fram sig från en sida till en annan genom knappar och backar bak med backpilarna i toppen. TabbedPage som är en meny som ligger i toppen på android och i botten på IOS mobiler. Slutligen finns CarouselPage som får dig byta från en sida till en annan med hjälp av swipes. Projektets applikation använde sig huvudsakligen av NavigationPage som grund och TabbedPage som huvudmeny.



Figur 3 är en bild tagen från microsofts egna hemsida som visar hur alla visual studio Xamarins olika designtyper ser ut för dess sidor.[13]

När det kommer till temat av designen så krävdes det att projektet var anpassningsbart för just volvos on call applikation. För att kunna identifiera alla färgerna, texttypsnitten, textstorlekarna och knapp designen så användes verktyget Figma för gränssnittsdesign (som man kan se på **Figur 4)** så att man sedan kunde tillämpa alla dessa egenskaperna på vår egna visual studio xamarin applikation. I detta fallet så användes exempelvis färgkoderna “#EDEDED” och “#FFFFFF” som bakgrundsfärg samt “Sans-Serif” som typsnitt för all standard text (**Figur 5)**.



Figur 4 är en skärmdump tagen på Figma appen som visar hur vi har med hjälp av en skärmdump tagen på “Volvo on call” menyn kunnat baklänges konstruera (reverse engineer) appens design tema.

```
62          <!-- TouchID login button -->
63          <StackLayout HeightRequest="150" Grid.Row="4"><!--BackgroundColor="#CFCFCF"-->
64              <Button Text="Sign in with TouchID"
65              ContentLayout="Top" Image="TouchID_icon.png" BackgroundColor="#EDEDED" FontSize="24" FontFamily="sans-serif"
66                  HeightRequest="150" Clicked="TouchIDButtonClickedAsync" VerticalOptions="CenterAndExpand">
67              </Button>
68          </StackLayout>
69          <!-- faceID login button. Add backgroundcolors to stacklayout and increase heigh on layout grid-4 to 152 and sta
70          <StackLayout HeightRequest="150" Grid.Row="5"> <!--BackgroundColor="#CFCFCF"-->
71          <Button Text="Sign in with FaceID"
72              ContentLayout="Top" Image="faceID_icon.png" BackgroundColor="#EDEDED" FontSize="24" FontFamily="sans-serif"
73                  HeightRequest="150" VerticalOptions="CenterAndExpand"
74                  Clicked="FaceIDButtonClicked">
75          </Button>
76      </StackLayout>
77      <!-- Manual login button -->
78      <StackLayout HeightRequest="110" Grid.Row="6">
79          <Button Text="Sign in manually"
80              ContentLayout="Top" Image="manual_icon.png" BackgroundColor="#EDEDED" FontSize="18" FontFamily="sans-serif"
81                  HeightRequest="110" VerticalOptions="CenterAndExpand"
82                  Clicked="ManualLoginButtonClicked">
83          </Button>
84      </StackLayout>
```

Figur 5 är en skärmdump som visar hur vi har lyckats använda “Volvo On Call” appens design tema på helt nya designade sidor med.

4.3.2 Implementering

För att kunna uppnå projektets mål så krävdes en utvecklingsmiljö som man kan skapa mobilapplikationen och dess funktionaliteter på, samt användning av

arbetsramverket scrum som är en effektiv och vanlig modell bland stora företagen för systemutveckling.

I arbetets implementering av scrum så användes mjukvaror som alla scrum-medlemmar kan dela information med. Exempel på dessa typer av mjukvaror är google drive som användes för att låta gruppen skriva planeringsrapporten och examens arbete rapporten.

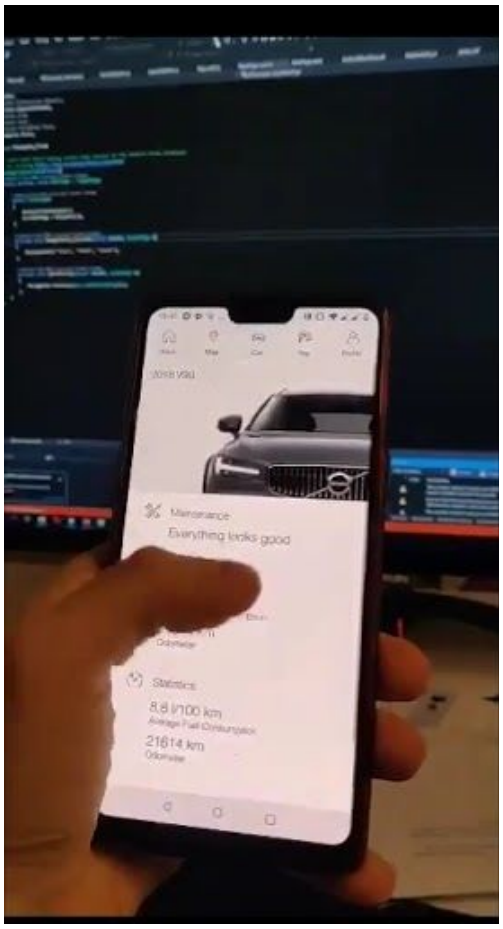
Ett annat exempel på en sådan mjukvara är whiteboard mjukvaran Trello som användes för att skapa en scrum board som alla inplanerade uppgifter och mål befinner sig vid. Utöver det så användes även webbhotellet Github för att låta gruppmedlemmarna dela programkoden och tilläggen för mobilapplikationen.

Med tanke på att biometrisk autentisering är en avancerad funktionalitet så krävs det en avancerad utvecklingsmiljö att utveckla appen på. Därför så är simpla prototyp utvecklingsmiljöer inte ett alternativ.

Utöver detta så var ett mål för projektets arbete att mobilappen både är kompatibel med android mobiler och med iphone mobiler. I normala fall då man vill utföra extremt avancerade funktionaliteter så skapas två liknande appar, ena i utvecklingsmiljön “Android Studio” och andra i utvecklingsmiljön “xCode”. Eftersom att mobilapplikationens funktionaliteter bara var någorlunda avancerade så utvecklades mobilapplikationen i utvecklingsmiljön “Visual Studio Xamarin” istället som tillät apputveckling i både android mobiler och iphone mobiler samtidigt.

För att kunna förbättra utvecklarnas arbetsupplevelse och utvecklingens effektivitet för gruppmedlemmarna så har ett par tillägg till “Visual Studio Xamarin” införts.

Vanligtvist så testas mobilapplikationen huvudsakligen med en långsam emulator som behövs köras igång varje gång appen testas. Detta har förenklats med ett tillägg som möjliggör att medlemmarna kan trådlöst kompilera mobilappen direkt till mobilen som man kan se i **Figur 6**. Detta är utfört med hjälp av windows egna Android Debug Bridge (ADB) som möjliggör en trådlöst USB uppkoppling över nätet. Utöver detta så användes också tillägget “Hot Reload”.



Figur 6 är ett foto taget på en av projektmedlemmarnas mobil då den trådlöst kompilerar mobilappen direkt ifrån utvecklingsmiljön “Visual Studio Xamarin”.

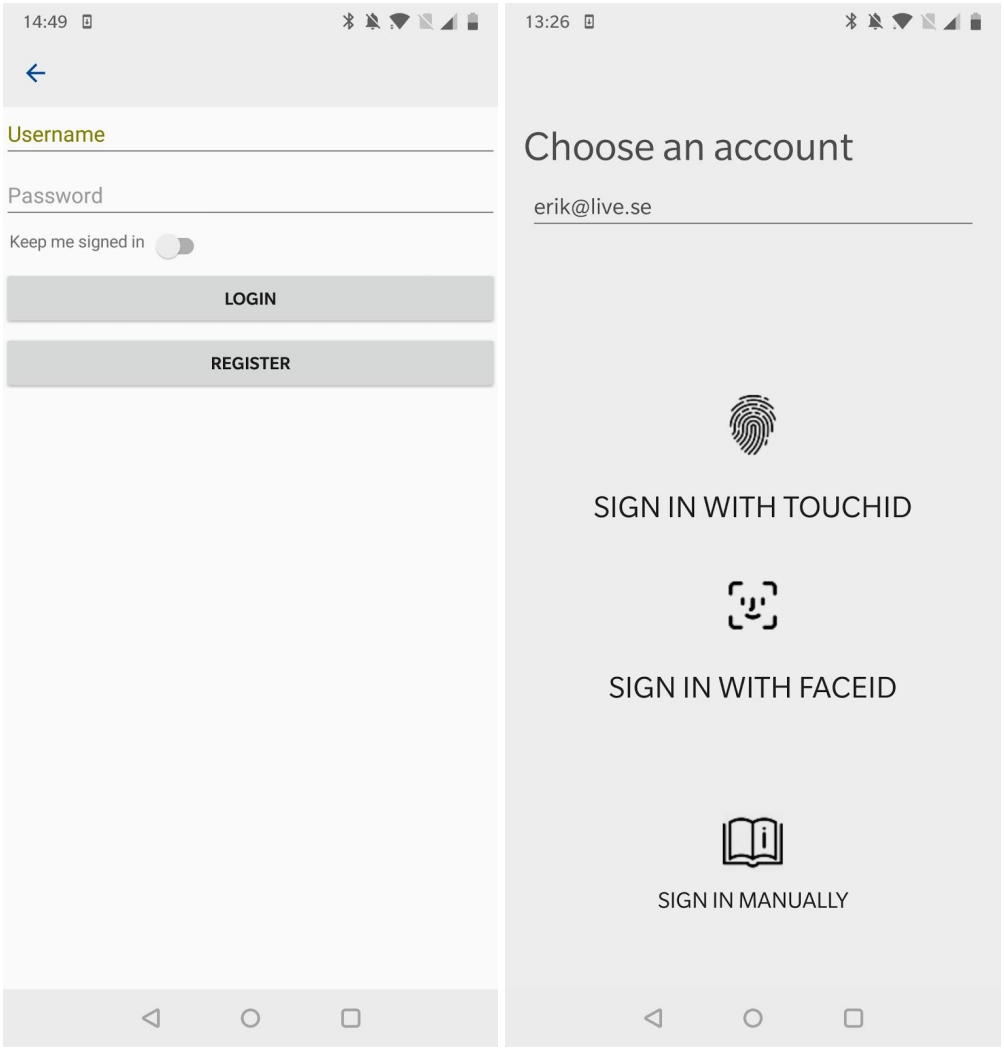
Med hjälp av dessa tillägg så utvecklades programkoden med en betydligt högre hastighet. En sida för en mobilapplikation som skulle kräva tiotals timmar att skapa kunde efter dessa tillägg bli utförda på mindre än ett par timmar.

Eftersom att vissa funktionaliteter både orsakar buggar och är komplicerade så användes ytterligare tillägg på Visual Studio Xamarin för att lösa det. Exempel på dessa tillägg är fingeravtrycksläsning, avancerad lista systemet och menyfältet som finns i applikationen.

5 Resultat

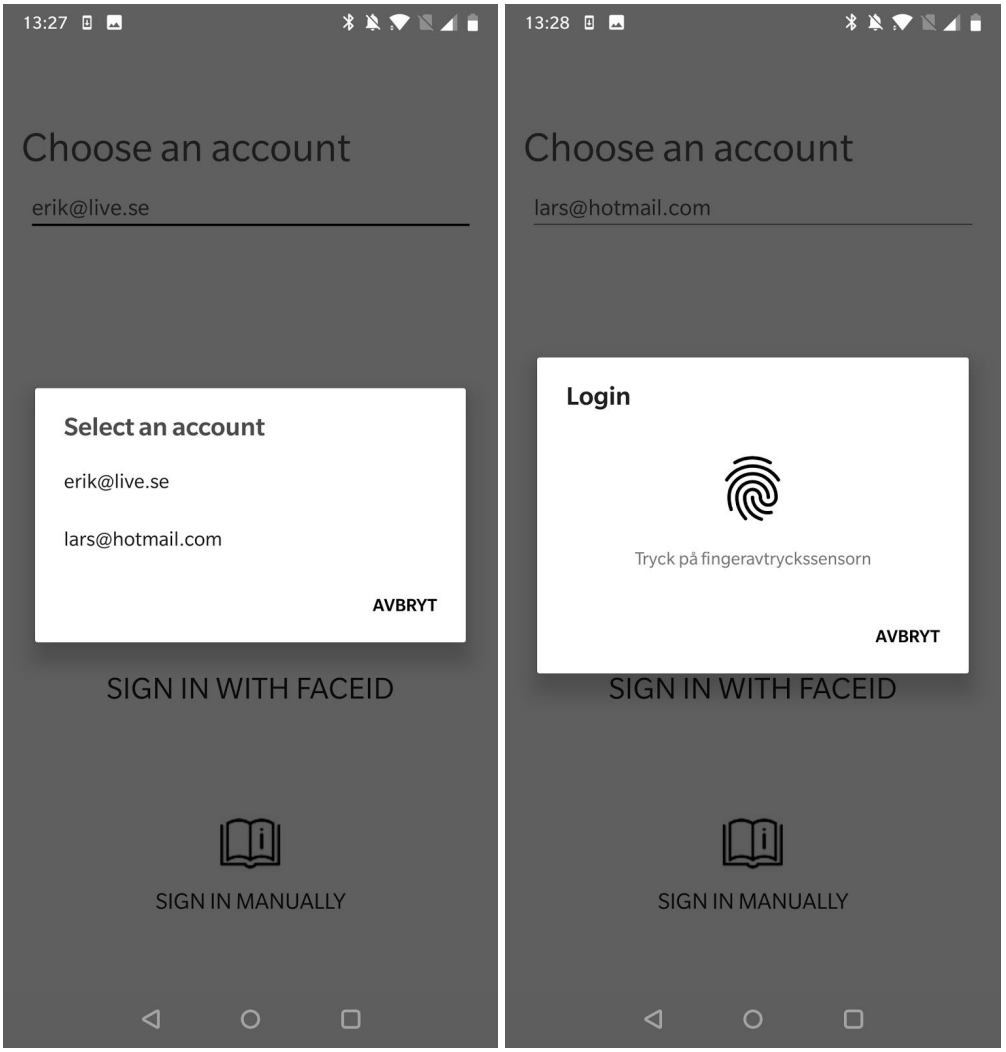
Som ett resultat av projektet så skapades en mobil IOS och Android applikation som har ett inloggningssystem kombinerat med single sign on och även multifaktor inloggningsalternativ som exempelvis fingeravtryckskläsning.

Då man inte har något konto sparat på applikationen så kommer man upp till menyn i **figur 7**, efter att man har loggat in och valt att spara användarnamnet och lösenordet så blir **Figur 8** den nya loginskärmen nästa gång man startar appen. I **figur 8** så är “Single Sign-on” tillgängligt vilket låter dig logga in på ditt konto utan att behöva skriva användarnamnet och lösenordet.



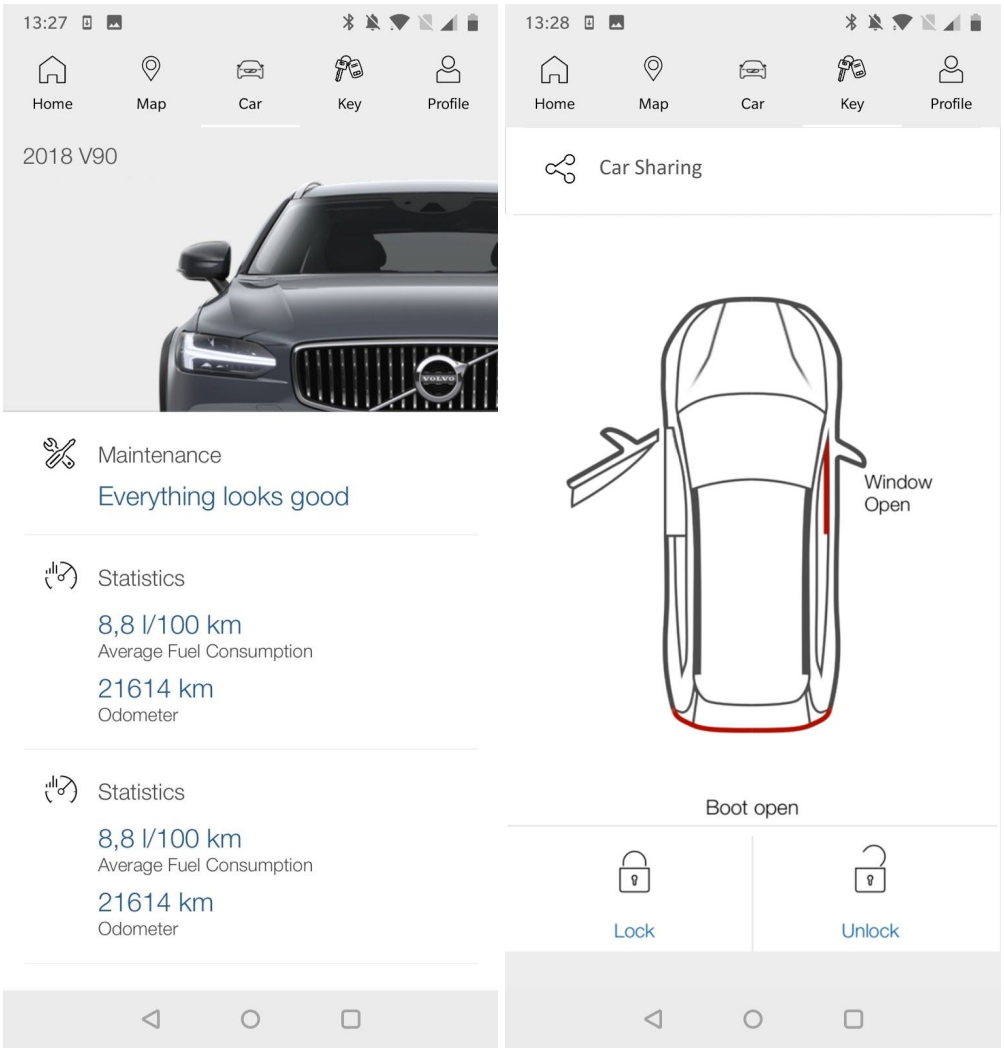
Figur 7 är en skärmdump på loginskärmen av vår app vilket är det första man ser då man har installerat applikationen. **Figur 8** är en skärmdump på multifaktor autentiserings loginskärmen av applikationen.

För att kunna låta en användare spara flera konton så finns det en ruta vid toppen av sidan som sedan leder en till menyn som finns i **Figur 9**, sedan så kan man med kontot välja att logga in med fingeravtrycksläsning som i **Figur 10**, ansiktsläsning (som inte är implementerat) eller manuellt med användarnamn och lösenord som i **Figur 7**.



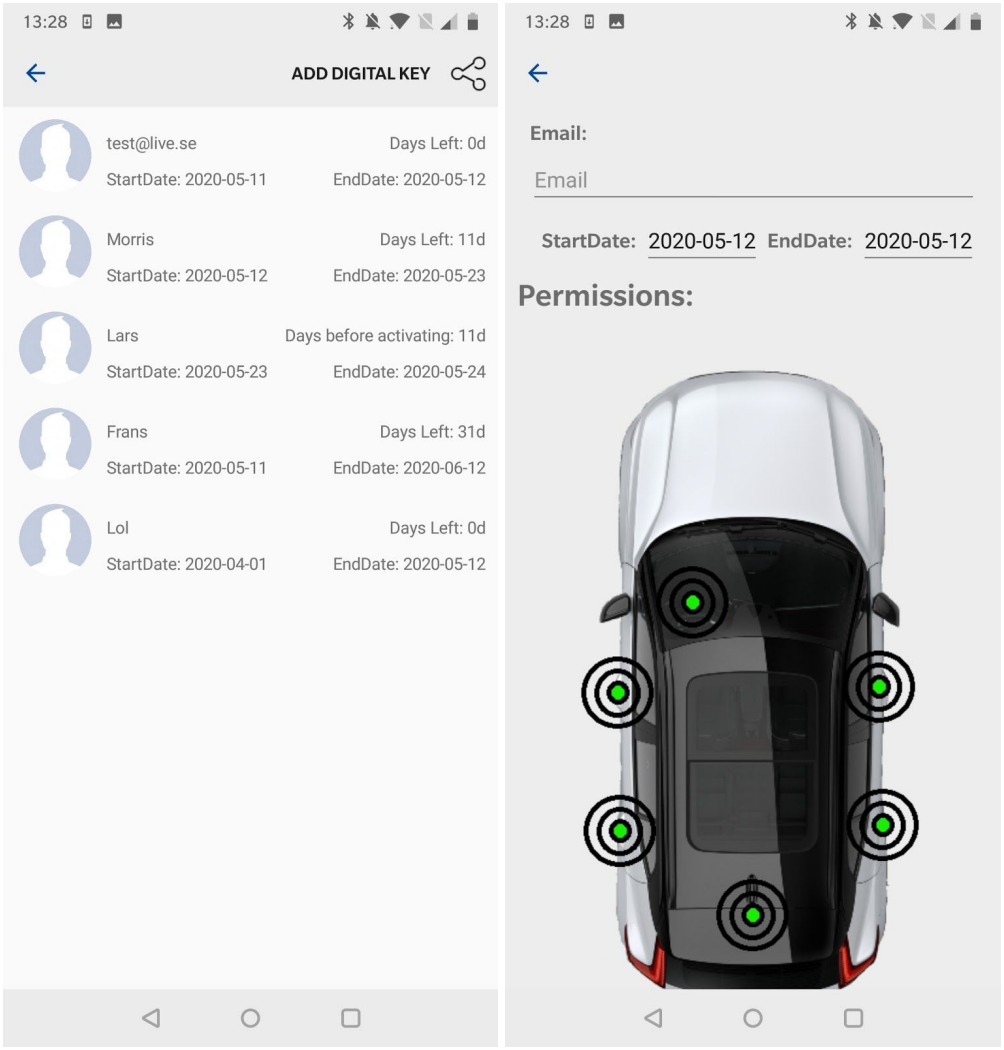
Figur 9 är en skärmdump som visar hur det ser ut då man får välja mellan flera konton som man kan logga in med. **Figur 10** är en skärmdump som visar hur inloggning med fingeravtrycksläsning ser ut.

Efter att man har loggat in så hamnar man i **Figur 11** och **Figur 12** som är en modifierad replika av Volvos “Volvo on call” app meny så att arbetet har ett realistiskt exempel på hur nyckel delningen kan se ut. Klickar man på “Car Sharing” knappen som finns i **Figur 12** (och **Figur 11** om man scrollar) så når man menyn för delning av bilnyckel som finns i **Figur 13**.



Figur 11 och **Figur 12** är ett par skärmdumpar tagna på vår replika av menyn från “Volvo on call” appen, utöver kopian så har vi dessutom infört en knapp för delning av bil som heter “Share a car”. Kopian av volvo on call menyn är gjort med hjälp av reverse engineering med Figma och Adobe XD för att få temat och sedan utförd med vår egna liknande design.

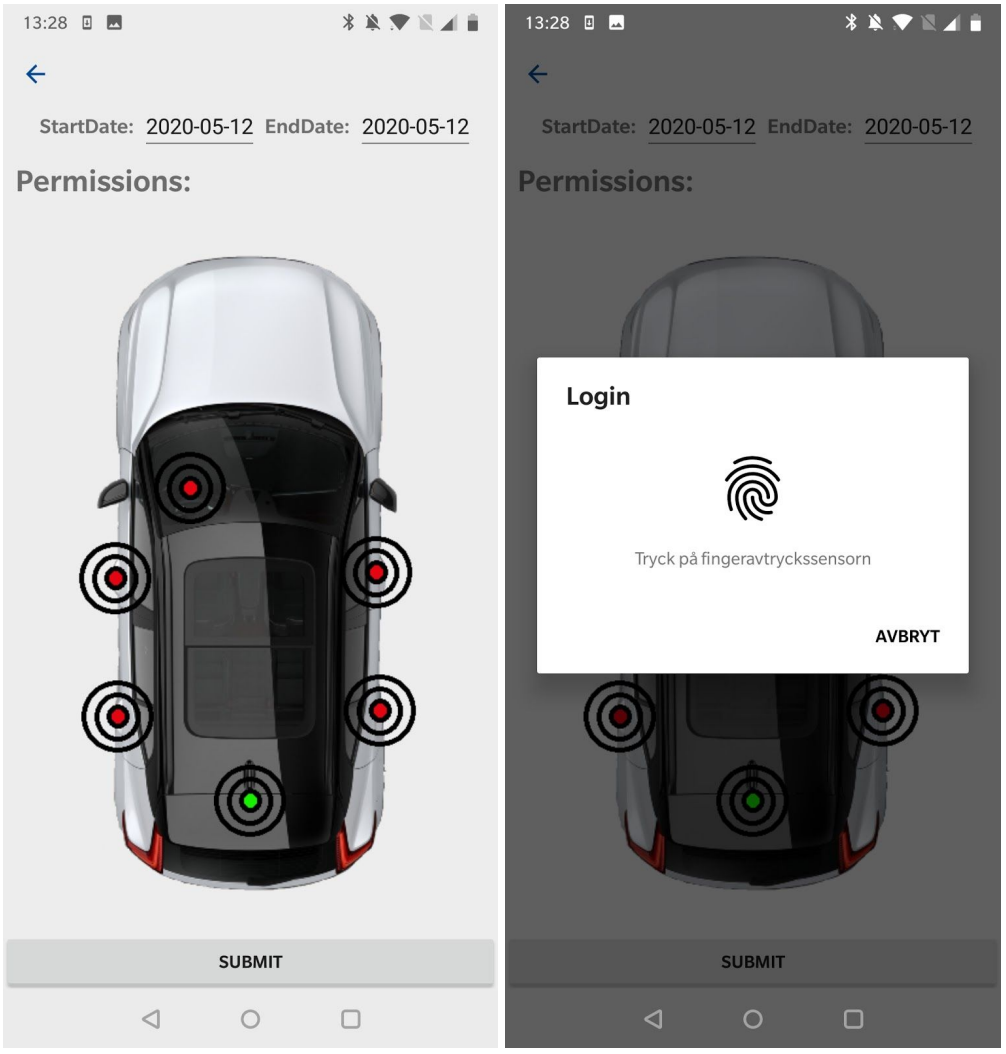
I menyn för delning av bilnyckel som finns i **Figur 13** så ser man alla nycklar som man har delat, datumet man gjorde det på och datumet som det slutar på. Man ser även antalet dagar som är kvar tills nyckeln går ut och om startdatumet inte har passerats än så visar den antalet dagar tills nyckeln aktiveras. Klickar man på “Add digital key” eller ikonen bredvid från **Figur 13** så når man **Figur 14** som är menyn för att lägga till nyckel.



Figur 13 är en meny för bildelning som visar alla nycklar som är delade till sin bild och **Figur 14** visar första halvan av tilläggs-menyn för ny nyckel.

I menyn för tillägg av bilnyckel så får du välja mailen eller användarnamnet av användaren du vill dela nyckeln med, startdatumet som nyckeln bör påbörja på och datumet som det inte är giltigt vid längre.

Till sist så får du välja vilka lås som du vill att den delade nyckeln skall få tillgång till, i **Figur 15** bilden nedan så har det exempelvist skapats en nyckel i 1 dag som bara har tillgång till bagageluckan på bilen. För att motverka otillåten bildelning när t.ex någon har loggat in på appen och lämnat mobilen så kommer en ytterligare fingeravtryckskläsning som man ser i **Figur 16**, har inte mobilen fingeravtryckskläsning tillgängligt så är det tänkt att en PIN förfrågan kommer upp istället.



Figur 15 är en skärmdump som visar tilläggs-menyn med införda inställningar där enbart bagageluckan är tillgänglig. **Figur 16** är en skärmdump som visar fingeravtryckskläsning konfirmering då man lägger till en nyckel så att inte någon ska kunna sno någon annans mobil och ge sig själv nyckeln.

6 Diskussion

6.1 Diskussion av resultat

Applikationens resultat blev att man kan autentisera en individ på ett enkelt och snabbt sätt utan att störa användaren för mycket. På grund av att vi valde biometrisk autentisering räcker det för användaren att sätta fingret på mobilens avläsare för att kunna verifiera sig, vilket inte tar mer än några sekunder. Hade vi istället valt att användaren måste skriva in lösenord varje gång denna vill dela sin nyckel hade det inte bara tagit mer tid, utan även varit en säkerhetsrisk eftersom ett stulet lösenord hade gett den obehöriga full tillgång till applikationen. Men med biometrisk autentisering som extra säkerhet så kan ett stulet lösenord bara logga in på kontot, men inte göra några känsliga handlingar utan att visa vem man är genom fingeravtryck, vilket är svårt att replikera.

I projektet så implementerades fingeravtrycksläsning som biometrisk autentisering, vilket valdes på grund av dess bra säkerhet. Det finns fler kroppsdelar man hade kunnat autentisera med som exempelvis ansiktet och ögonen för att variera, men det ansågs inte nödvändigt för detta projekt eftersom målet var att det skulle vara enkelt för användaren och för många alternativ kan lätt bli överväldigande för en ny användare. Dessutom var androids ansiktsläsning inte optimal för säkerheten vilket vi valde att inte kompromissa med(se 2.3.1). Design för inloggning med ansiktsläsning togs dock med som ett visuellt exempel hur det kan se ut om funktionen sen implementeras (se **figur 8** i resultat).

6.2 Genomförande och fortsatt arbete

I arbetet så var tanken att använda scrum som arbetsmetod, vilket det gjordes med utvärderingsmöten varje två och en halv veckas intervall. På mötena gick vi igenom vad vi gjort vilket gav regelbunden feedback hur arbetet gick och vad man kunde förbättra. Allt med scrum togs dock inte med som exempelvis dagliga scrum möten, det togs inte med på grund av att arbetet bestod av bara två personer och därför behövde inte arbetet synkroniseras lika ofta som om det hade varit en större grupp. Roller inom scrum som produktägare och scrum master togs heller inte med på grund av gruppens storlek. Den regelbundna feedbacken vi fick från mötena var en stor fördel eftersom det hjälpte arbetet i rätt riktning och svarade på eventuella frågor gruppen hade.

Eftersom att den största faktorn som stoppade arbetet ifrån att implementera fler funktioner var tidsbrist, så hade det varit viktigt för gruppen att utföra åtgärder som hade sparat gruppen tid. En åtgärd som hade sparat tid hade varit att analysera och jämföra verktygen som var tänkta att användas i början av projektet med andra alternativ för att snabbare kunna hitta de bästa. Detta är viktigt eftersom att det ger projektmedlemmarna en chans att se de möjligheterna som handledaren rekommenderar jämfört med andra alternativ.

Ett exempel på ett fall som vi inte lyckades med detta på är då projektgruppen blev rekommenderade att använda externa applikationen PingID vid hantering av fingeravtrycksläsning och ansiktsläsning. På grund av att PingID hade ändrat sitt system för utdelning av gratisversion och att gruppen hade fokuserat sig på vad PingID är och inte på hur det fungerar så kostade det 6 veckor bara för att inse vid implementationen att det var svårt att implementera PingID med gratisversionen.

Ett annat exempel på detta är att vi inte var medvetna om att det krävdes en MAC dator för att kunna testa en mobilapplikation på Iphone, orsaken bakom detta var att gruppmedlemmarna inte hade analyserat hur “Visual Studio Xamarin” tillräckligt i början. På grund av detta så kostade det projektmedlemmarna en ytterligare vecka värt av planeringar bara för att försöka finna en idé på hur projektmedlemmarna kan få IOS versionen av mobilapplikationen att fungera. Vid fortsatt arbete hade effektiviteten och kvaliteten på applikationen förbättras om man haft dessa problem i åtanke.

Något som vi hade kunnat tagit med och funderade på att göra i applikationen för att förbättra säkerheten med MFA var anpassningsbar autentisering, det vill säga antalet verifieringar ändras beroende på situationen. Exempel på detta vi kunde valt är att användaren kan tvingas verifiera sig en extra gång ifall individen är utomlands eller om användaren använder en ny enhet från tidigare inloggningar. Dessa implementeringar hade lett till en ökad säkerhet utan att störa upplevelsen för användaren vilket var i linje med projektets mål och skulle vid en vidareutveckling på projektet vara en prioritet.

6.3 Miljö

En miljöaspekt som är positiv är att om mer personer använder digitala nycklar i sin mobil så minskar behovet av fysiska nycklar, vilket leder till mindre producering av nycklar och i sin tur kan minska utsläppen.

6.4 MFA i framtiden

Vi tror att nästa framsteg inom digitaliseringen är en framtid med en autentisering fri från lösenord[7], främst för den ökade säkerheten men även på grund av andra faktorer. För det första så är det bra för användarupplevelsen och därmed bättre för kunden, kunden behöver exempelvis inte komma ihåg orimligt många lösenord som man behöver vid användning av flera konton idag. Samt kan det vara bra ur ett ekonomiskt perspektiv eftersom anställda världen över spenderar tid på att skriva in och komma ihåg lösenord och på lång sikt kan leda till en förlust av inkomst eftersom inget arbete utförs. Med en snabbare inloggning kan den tiden gå åt till arbete istället och leda till större inkomst för företaget.

Alla dessa faktorer kan uppfyllas med multifaktor autentisering eftersom med MFA så kan man få den förbättrade säkerheten utan att behöva använda sig av vanliga lösenord genom att ha andra typer av verifieringar som biometrisk autentisering till exempel. Då går det även snabbare att verifiera sig vilket förbättrar kundens upplevelse samt kan spara både tid och pengar.

7 Slutsats

Autentisering är en viktig del av vardagen idag och kommer att bli ännu viktigare eftersom att samhället blir allt mer digitaliserat och säkerhetsbristerna med vanliga lösenord kommer allt mer i fokus. Brister i säkerheten kan kosta företagen stora mängder pengar och borde därför vara en hög prioritet på just säkerheten. Med resultatet i detta arbete har vi sett att man kan använda andra typer av autentiseringar än enbart lösenord samt öka antalet av dem med MFA, utan att det förstör användarupplevelsen.

Vill man göra det ännu säkrare kan anpassningsbar autentisering implementeras vilket diskuterades i diskussion, samt byta ut alternativet att logga in med vanligt lösenord mot ett säkrare sätt som engångskod eller annan typ av biometrisk autentisering som exempelvis ansiktsläsning, möjligheterna är många med multifaktor autentisering.

Sammanfattningsvist så har projektet nått sitt slutgiltiga mål, det har uppkommit hinder och avgränsningar genom arbetsgången men i slutändan så skapades det en mobilapplikation med fokus på användarvänlighet och säkerhet. I applikationen finns MFA alternativ i kombination med ett system som möjliggör modifierad delning av bilnycklar genom mobilen.

Bortsett från målen så har projektmedlemmarna även fått erfarenhet av att skapa mobil-applikationer på ett effektivt sätt, använda ramverket scrum och har lärt sig tekniker för att både effektivisera arbetet och för att göra arbetet mer intressant.

Referenser

[1] LastPass by LogMeIn, THE 3RD ANNUAL GLOBAL PASSWORD SECURITY REPORT.
Tillgänglig: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LMI0828a-IAM-LastPass-State-of-the-Password-Report.pdf

[2] Alex Hunter, Why Biometric Authentication is Better than Passwords by Alex Hunter, Hakin9.
Tillgänglig: https://hakin9.org/why-biometric-authentication-is-better-than-passwords/

[3] Biometric Authentication:What Consumers Want, Veridium.
Tillgänglig: https://info.veridiumid.com/biometrics-what-consumers-want

[4] Volvo In-car Delivery - beställ på nätet och få leverans direkt till din bil, Rejmes.
Tillgänglig:https://rejmes.se/nyheter/volvo-in-car-delivery-bestall-pa-natet-och-fa-leverans-direkt-till-din-bil

[5] Gabriel Nica, Video: Here's How the BMW Digital Key Works, BMWBLOG.
Tillgänglig: https://www.bmwblog.com/2018/11/17/video-heres-how-the-bmw-digital-key-works/

[6] Infotainment, Audi Mediacenter.
Tillgänglig: https://www.audi-mediacenter.com/en/technology-lexicon-7180/infotainment-7183

[7] Andrew Shikiar & Adrien Ogee, Passwordless Authentication The next breakthrough in secure digital transformation, World Economic Forum.
Tillgänglig: http://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf

[8] Nicholson, Coventry & Briggs, Age-Related Performance Issues for PIN and Face-Based Authentication Systems, CHI 2013: Changing Perspectives.
Tillgänglig: https://dl.acm.org/doi/pdf/10.1145/2470654.2470701

[9] Olabode Anise & Kyle Lady, State of the Auth Experiences and Perceptions of Multi-Factor Authentication, Duo Security.
Tillgänglig: https://duo.com/assets/ebooks/state-of-the-auth.pdf

[10] Das, Sanchari & Wang, Bingxing & Tingle, Zachary & Camp, L.. (2019). Evaluating User Perception of Multi-Factor Authentication: A Systematic Review.

[11] Sharp, Helen, et al. Interaction Design : Beyond Human-Computer Interaction, John Wiley & Sons, Incorporated, 2019. ProQuest Ebook Central, page 26.

[12] Sharp, Helen, et al. Interaction Design : Beyond Human-Computer Interaction, John Wiley & Sons, Incorporated, 2019. ProQuest Ebook Central, page 20.

[13] Xamarin.Forms Navigation, Microsoft.
Tillgänglig: https://docs.microsoft.com/en-us/xamarin/xamarin-forms/app-fundamentals/navigation/

[14] 2017 Data Breach Investigations Report 10th Edition, Verizon.

Tillgänglig: https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

[15]2020 Data Breach Investigations Report, Verizon.

Tillgänglig:
https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

[16] JV Chamary,How Face ID Works On iPhone X, Forbes

https://www.forbes.com/sites/jvchamary/2017/09/16/how-face-id-works-apple-iphone-x/#e2a5244624db

[17]Richard Chirgwin,Full frontal vulnerability: Photos can still trick, unlock Android mobes via facial recognition, The Register.
Tillgänglig: https://www.theregister.com/2019/01/04/photos_trick_smartphones/