Sikkerhed i macOS

Oversigt for IT-afdelingen

Apple har designet macOS-platformen med en integreret tilgang til hardware, software og tjenester, som giver indbygget sikkerhed og gør platformen nem at konfigurere, implementere og administrere. macOS indeholder de vigtige sikkerhedsteknologier, som IT-medarbejdere skal bruge til at beskytte data og integrere løsninger i sikre virksomhedsnetværk. Apple har desuden samarbejdet med organer for standarder for at sikre, at platformen lever op til de nyeste sikkerhedscertificeringer. Denne oversigt forklarer kort nogle af disse funktioner.

Dette dokument er inddelt i følgende emneområder:

- **Systemsikkerhed:** Den integrerede og sikre software, der danner grundlaget for macOS.
- **Kryptering og databeskyttelse:** Arkitekturen og design, der beskytter brugerdata, hvis enheden bliver væk eller stjålet.
- **App-sikkerhed:** Systemerne, der beskytter Mac-computeren mod malware og gør det muligt at køre programmer sikkert, uden at det går ud over platformens integritet.
- **Godkendelse og digital signering:** Funktionerne i macOS til administration af brugeroplysninger og understøttelse af industristandardteknologier såsom smart cards og S/MIME.
- **Netværkssikkerhed:** Branchens standard for netværksprotokoller, der giver sikker godkendelse og kryptering af data under overførsel.
- **Kontrol af enheder:** Metoder, som gør det muligt at administrere Apple-enheder, forhindre uautoriseret brug og udføre ekstern sletning, hvis en enhed bliver væk eller stjålet.

Læs mere om macOS-implementering og -administration i macOS – Håndbog om implementering på help.apple.com/deployment/macos.

Læs mere om sikkerhedsfunktioner i Apple-tjenester, som ikke er beskrevet i dette dokument, i vejledningen "iOS-sikkerhed" her www.apple.com/dk/business/docs/iOS_Security_Guide.pdf.

Systemsikkerhed

macOS-systemsikkerhed er designet, så både software og hardware er sikker på tværs af alle kernekomponenter i hver enkelt Mac-computer. Denne arkitektur er central for sikkerheden i macOS og kommer aldrig i vejen for enhedens anvendelighed.

UNIX

macOS-kernen – styresystemets midtpunkt – er baseret på BSD (Berkeley Software Distribution) og Mach-mikrokernen. BSD leverer det grundlæggende filsystem

og netværkstjenester, en ordning til at identificere brugere og grupper samt mange andre centrale funktioner. BSD begrænser desuden adgangen til filer og systemressourcer baseret på bruger- og gruppe-id'er.

Mach sørger for hukommelsesadministration, trådkontrol, hardwareabstraktion og kommunikation mellem processer. Mach-porte repræsenterer opgaver og andre ressourcer og giver adgang til portene ved at kontrollere, hvilke opgaver der kan sende en meddelelse til dem. BSD-systemets sikkerhedspolitikker og Mach-adgangstilladelserne udgør grundlaget for sikkerheden i macOS og er afgørende for at forstærke den lokale sikkerhed.

Kernens sikkerhed er afgørende for hele styresystemets sikkerhed. Kodesignering beskytter kernen og kerneudvidelser fra tredjeparter samt andre systembiblioteker og eksekverbare filer, der er udviklet af Apple.

Model for brugertilladelse

Et vigtigt aspekt af Mac-sikkerheden er funktionen, hvor der gives eller nægtes adgangstilladelser (også kaldet adgangsrettigheder). En tilladelse er muligheden for at udføre en bestemt handling, f.eks. at få adgang til data eller til at køre kode. Der gives tilladelser til mapper, undermapper, filer og programmer samt for specifikke data i filer, app-funktioner og administrative funktioner. Digitale signaturer identificerer adgangsrettighederne til programmer og systemkomponenter.

macOS kontrollerer tilladelser på mange niveauer, f.eks. Mach- og BSD-komponenterne i kernen. Tilladelser til netværksprogrammer kontrolleres med netværksprotokoller i macOS.

Obligatorisk adgangskontrol

macOS anvender desuden obligatorisk adgangskontrol – politikker for sikkerhedsbegrænsninger, som laves af udvikleren og ikke kan tilsidesættes. Denne tilgang adskiller sig fra skønsmæssig adgangskontrol, hvor brugerne kan tilsidesætte politikker alt efter deres præferencer. Obligatorisk adgangskontrol er ikke synlig for brugerne. Men de udgør den underliggende teknologi, som gør det muligt at aktivere flere forskellige vigtige funktioner, bl.a. sandboxing, børnesikring, udvidelser og beskyttelse af systemets integritet.

Beskyttelse af systemets integritet

OS X 10.11 eller nyere indeholder beskyttelse på systemniveau, kaldet Beskyttelse af systemets integritet (SIP), som skrivebeskytter komponenter på visse kritiske områder i filsystemet for at forhindre, at de køres eller modificeres af ondsindet kode. Beskyttelse af systemets integritet er en computerspecifik indstilling, der som standard er aktiveret, når du opgraderer til OS X 10.11. Hvis den deaktiveres, forsvinder beskyttelsen for alle partitioner på den fysiske lagerenhed. macOS anvender denne sikkerhedspolitik på alle processer, der køres i systemet – uanset om de kører i en sandbox eller med administrative rettigheder.

Læs mere om disse skrivebeskyttede områder af filsystemet i supportartiklen fra Apple "Om Beskyttelse af systemets integritet" på support.apple.com/HT204899.

Kerneudvidelser

macOS har en mekanisme til kerneudvidelser, som giver mulighed for dynamisk indlæsning af kode i kernen, uden at det er nødvendigt at omkompilere eller omlinke. Da disse kerneudvidelser (KEXT) både tilbyder modularitet og dynamisk indlæsning, udgør de et naturligt valg for alle relativt selvstændige tjenester,

som kræver adgang til interne kernegrænseflader, f.eks. hardwareenhedsdrivere eller VPN-programmer.

Med henblik på at forbedre sikkerheden i Mac-computeren kræves der brugertilladelse for at indlæse kerneudvidelser, der installeres sammen med eller efter installationen af macOS High Sierra. Dette er kendt som brugergodkendt indlæsning af kerneudvidelser. Alle brugere kan godkende en kerneudvidelse, selv hvis de ikke har administrative rettigheder.

Kerneudvidelser kræver ikke godkendelse, hvis de:

- Blev installeret på Mac-computere, inden der blev opgraderet til macOS High Sierra.
- Erstatter tidligere godkendte udvidelser.
- Kan indlæses uden brugertilladelse ved at bruge kommandoen `spctl`, som bliver tilgængelig ved start fra macOS-gendannelsespartitionen.
- Kan indlæses via MDM-konfigurationen (Administration af mobile enheder). I macOS High Sierra 10.13.2 og nyere kan du bruge MDM til at specificere en liste over kerneudvidelser, der kan indlæses uden brugertilladelse. Denne mulighed kræver, at en Mac-computer kører macOS High Sierra 10.13.2, som er blevet registreret i MDM enten via Tilmeldingsordningen for enheder (Device Enrolment Program, DEP) eller via brugergodkendt MDM-tilmelding.

Læs mere om kerneudvidelser i supportartiklen fra Apple "Prepare for changes to kernel extensions in macOS High Sierra" på support.apple.com/HT208019.

Firmware-adgangskode

macOS tillader brugen af en adgangskode for at forhindre uønskede modifikationer af firmware-indstillinger i et bestemt system. Denne firmware-adgangskode bruges til at forhindre følgende:

- Start fra en uautoriseret systemenhed
- Ændringer af startprocessen, f.eks. start i enkeltbrugertilstand
- Uautoriseret adgang til macOS-gendannelse
- Direct Memory Access (DMA) gennem grænseflader såsom Thunderbolt
- Ekstern harddisk, som kræver DMA

Bemærk: T2-chippen fra Apple i iMac Pro forhindrer brugere i at nulstille firmware-adgangskoden, selv hvis de får fysisk adgang til Mac-computeren. På en Mac-computer uden T2-chippen skal der træffes yderligere sikkerhedsforanstaltninger for at forhindre brugere i at få fysisk adgang til Mac-computerens interne dele.

Internetgendannelse

Mac-computere, som ikke kan starte fra det indbyggede gendannelsessystem, forsøger automatisk at starte fra macOS-gendannelse over internettet. Når dette sker, vises der en roterende globus i stedet for et Apple-logo under start. Ved gendannelse kan brugere geninstallere den nyeste version af macOS eller den version, der blev leveret med den nuværende Mac-computer.

macOS-opdateringer bliver distribueret gennem App Store og gennemføres af macOS-installationsprogrammet, som ved hjælp af kodesignaturer kontrollerer integriteten og autenciteten af installationsprogrammet og dets pakker inden installationen. Tjenesten til gendannelse via internettet er desuden den officielle kilde til det styresystem, der blev leveret med en bestemt Mac-computer.

Læs mere om macOS-gendannelse i supportartiklen fra Apple "Om macOS-gendannelse" på support.apple.com/HT201314.

Kryptering og databeskyttelse

Apples filsystem

Apple File System (APFS) er et nyt moderne filsystem til macOS, iOS, tvOS og watchOS. Filsystemet er optimeret til flash-/SSD-lagring og har stærk kryptering, copy-on-write-metadata, deling af områder, kloning af filer og biblioteker, snapshots, hurtig størrelsesændring af biblioteker, atomic safe-save primitives og forbedringer i det grundlæggende filsystem samt et unikt copy-on-write-design, der bruger I/O-coalescing for at levere en maksimal ydeevne, mens datapålideligheden sikres.

APFS tildeler diskplads efter behov. Når en enkelt APFS-beholder har adskillige enheder, deles beholderens ledige plads og kan tildeles til en hvilket som helst af enhederne efter behov. Hver enhed bruger kun en del af den samlede beholder, så den tilgængelige plads er beholderens samlede størrelse minus den anvendte plads i alle beholderens enheder.

I macOS High Sierra skal en gyldig APFS-beholder indeholde mindst tre volumener, hvoraf de to første er skjult fra brugeren:

- Preboot-enhed: Indeholder de nødvendige data for at starte hver systemenhed i beholderen.
- Gendannelsesenhed: Indeholder gendannelsesdisken.
- Systemenhed: Indeholder macOS og Bruger-mappen.

FileVault

På hver Mac-computer findes der en indbygget krypteringsfunktion – FileVault – som beskytter alle data i hvile. FileVault bruger XTS-AES-128-datakryptering til at sikre data på en Mac-computer i hvile. Krypteringen kan bruges til at beskytte hele enheder på interne og eksterne lagringsenheder. Hvis en bruger indtaster et Apple-id og en adgangskode under indstillingen, foreslår Indstillingsassistenten at aktivere FileVault og lagre gendannelsesnøglen i iCloud.

En bruger, som aktiverer FileVault på en Mac-computer, bliver bedt om at levere gyldige brugeroplysninger, inden der fortsættes til startprocessen og gives adgang til specielle starttilstande, som f.eks. Computer som ekstern harddisk. Hvis brugeren ikke har gyldige brugeroplysninger eller en gendannelsesnøgle, bliver hele enheden ved med at være krypteret og beskyttet mod uautoriseret adgang, selv hvis den fysiske lagringsenhed fjernes og sluttes til en anden computer.

IT-afdelingen bør definere og håndhæve FileVault-konfigurationspolitikker via MDM med henblik på at beskytte data i virksomhedsmiljøet. Organisationer kan vælge mellem forskellige muligheder til at administrere krypterede enheder, såsom gendannelsesnøgler til virksomheden, personlige gendannelsesnøgler (der valgfrit kan deponeres med MDM) eller en kombination af begge. Nøglerotation kan også indstilles som en politik i MDM.

Krypterede diskbilleder

I macOS fungerer krypterede diskbilleder som sikre beholdere, hvor brugerne kan lagre eller overføre følsomme dokumenter og andre filer. Krypterede diskbilleder skabes med brug af Diskværktøj, om er placeret under /Programmer/Hjælpeprogrammer/. Diskbilleder kan enten krypteres ved hjælp af 128 bit eller 256 bit AES-kryptering. Eftersom et monteret diskbillede bliver behandlet

som en lokal enhed forbundet til en Mac-computer, kan brugere kopiere, flytte og åbne filer og mapper, som er lagret på den. Ligesom det er tilfældet med FileVault, bliver diskbilledets indhold krypteret og dekrypteret i realtid. Med krypterede diskbilleder kan brugere let udveksle dokumenter, filer og mapper ved at gemme et krypteret diskbillede på et flytbart medie, sende det som et bilag i en mail eller ved at gemme det på en fjernserver.

ISO 27001- og 27018-certificeringer

Apple er ISO 27001- og ISO 27018-certificeret for det system, der håndterer informationssikkerhed i forbindelse med infrastruktur, udvikling og aktiviteter, som understøtter disse produkter og tjenester: Apple School Manager, iCloud, iMessage, FaceTime, administrerede Apple-id'er og iTunes U, i overensstemmelse med Statement of Applicability v2.1 fra d. 11. juli 2017. Apples overholdelse af ISO-standarden blev certificeret af British Standards Institution (BSI). ISO 27001- og ISO 27018-overensstemmelsescertifikaterne kan læses på BSI's website:

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=apple&licencenumber=IS+649475

www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/search-results/?searchkey=company=Apple&licencenumber=PII%20673269

Kryptografisk godkendelse (FIPS 140-2)

De kryptografiske moduler i macOS er blevet godkendt i henhold til de amerikanske FIPS-standarder (Federal Information Processing Standards) 140-2 niveau 1 efter hver version siden OS X 10.6. Som med enhver stor lancering sender Apple modulerne til CMVP til revalidering, når Mac-styresystemet lanceres. Dette program validerer integriteten af kryptografiske aktiviteter for Apple-programmer og programmer fra tredjeparter, der bruger krypteringstjenester og godkendte algoritmer i macOS på korrekt måde. Alle Apples FIPS 140-2-overensstemmelsescertifikater kan læses på CMVP-leverandørsiden. CMVP har to forskellige lister med valideringsstatus for kryptografiske moduler afhængigt af deres aktuelle status på csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria Certification (ISO 15408)

Apple har tidligere fået macOS-certificeringer under Common Criteria Certification-programmet og skal til at gennemføre en evaluering af macOS High Sierra ud fra Operating System Protection Profile (PP_OSv4.1). Apple arbejder løbende med at evaluere og forsøge at opnå certificeringer ud fra nye og opdaterede versioner af cPP-profiler (Collaborative Protection Profiles), der findes i dag. Apple spiller en aktiv rolle inden for International Technical Community (ITC) i udviklingen af cPP-profiler med fokus på evaluering af vigtige sikkerhedsfunktioner til mobile enheder.

Sikkerhedscertificeringer, -programmer og -vejledning

Apple har arbejdet sammen med myndigheder i hele verden om at udvikle vejledninger, der indeholder anvisninger og anbefalinger til udviklingen af et mere sikkert miljø, også kendt som "device hardening" til meget udsatte miljøer. Disse vejledninger giver definerede og udførlige oplysninger om, hvordan funktioner i macOS konfigureres og anvendes med henblik på en forbedret beskyttelse.

Få de nyeste oplysninger om sikkerhedscertificeringer, godkendelser og vejledning til macOS i Apples supportartiklen "Produktsikkerhedscertificeringer, godkendelser og vejledning til macOS" på support.apple.com/HT201159.

Programsikkerhed

macOS indeholder indbyggede teknologier, som sikrer, at der kun installeres pålidelige programmer, for at beskytte mod malware. Pålidelige programmer beskyttes under brug takket være sikkerhed i flere lag i macOS, og programsignering sørger for, at programmerne ikke kan ændres.

Gatekeeper

macOS indeholder en funktion kaldet Gatekeeper, der kontrollerer, hvilke kilder programmer kan installeres fra. Med Gatekeeper kan brugere og organisationer indstille et påkrævet sikkerhedsniveau til installation af programmer.

Med den mest sikre Gatekeeper-indstilling kan brugere kun installere signerede programmer fra App Store. Standardindstillingen giver brugerne mulighed for at installere programmer fra App Store og programmer signeret med et gyldigt udvikler-id. Denne signatur indikerer, at programmer er blevet signeret af et certifikat udstedt af Apple, og at de ikke er blevet modificeret siden. Gatekeeper kan også deaktiveres helt efter behov gennem en Terminal-kommando.

I visse tilfælde anvender Gatekeeper randomiserede stier, bl.a. når programmer lanceres direkte fra et usigneret diskbillede eller fra et sted, hvor de blev downloadet og automatisk ikke blev gemt. Randomisering af stier gør programmer tilgængelige fra en uspecificeret skrivebeskyttet placering i filsystemet inden lancering. Dette forhindrer, at programmer tilgår kode eller indhold ved hjælp af relative stier. Det forhindrer dem desuden i at opdatere automatisk, hvis de lanceres fra denne skrivebeskyttede placering. Når Finder bruges til at f.eks. at flytte et program til mappen Programmer, betyder det, at randomiseringen af stier ikke længere vil blive anvendt.

Den største fordel ved denne standardsikkerhedsmodel er, at den tilbyder en bred beskyttelse af økosystemet. Hvis en malware-udvikler stjæler eller på anden vis får adgang til signering med et udvikler-id og bruger det til at distribuere malware, kan Apple hurtigt reagere og tilbagekalde signeringscertifikatet. Dermed stopes malwaren i at sprede sig yderligere. Denne type beskyttelse undergraver den økonomiske model af de fleste malware-kampagner på Mac-computeren og giver en omfattende beskyttelse til alle brugere.

Brugerne kan midlertidigt tilsidesætte disse indstillinger for at installere et hvilket som helst program. Organisationer kan bruge deres MDM-løsning til at etablere og håndhæve Gatekeeper-indstillinger samt til at tilføje certifikater til macOS-tillidspolitikken til evaluering af kodesignering.

XProtect

macOS indeholder indbygget teknologi til den signaturbaserede detektion af malware. Apple holder øje med, om der opstår nye malwareinfektioner og virus. Signaturerne i XProtect opdateres automatisk og uafhængigt af systemopdateringer – for at hjælpe med at beskytte Mac-systemer mod malwareinfektioner. XProtect detekterer og blokerer automatisk for installationen af kendt malware.

Værktøj til fjernelse af malware

macOS indeholder også teknologi, som udbedrer infektioner, hvis det skulle lykkedes for malware at trænge ind i en Mac-computer. Ud over at holde øje med malware-aktiviteter i økosystemer for at kunne tilbagekalde udvikler-id'er (hvis relevant) og udstede XProtect-opdateringer udsteder Apple også opdateringer til macOS for at fjerne malware fra berørte systemer, der er

konfigureret til at modtage automatiske sikkerhedsopdateringer. Når værktøjet til fjernelse af malware modtager opdaterede oplysninger, bliver malwaren fjernet efter den næste genstart. Værktøjet til fjernelse af malware genstarter ikke automatisk Mac-computeren.

Automatiske sikkerhedsopdateringer

Apple udsteder automatisk opdateringerne til XProtect og værktøjet til fjernelse af malware. Som standard søger macOS efter denne type opdateringer hver dag. Få yderligere oplysninger om automatiske sikkerhedsopdateringer i supportartiklen fra Apple "Mac App Store: Automatiske sikkerhedsopdateringer" på support.apple.com/HT204536.

Beskyttelse ved programafvikling

Systemfiler, ressourcer og kernen er afskærmet fra brugerens programområde. Alle programmer fra App Store er "sandboxed", så de ikke kan få adgang til data, der er lagret af andre programmer. Hvis et program fra App Store skal have adgang til data fra et andet program, kan det kun ske ved hjælp af API'erne og tjenesterne fra macOS.

Obligatorisk programkodesignering

Alle programmer fra App Store er signeret af Apple for at sikre, at de ikke er blevet modificeret eller ændret. Apple signerer alle programmer, der leveres med Apple-enheder. Mange af de programmer, der distribueres uden for App Store, bliver signeret af udvikleren ved hjælp af et Apple-udstedt certifikat for udvikler-id (kombineret med en privat nøgle) for at køre under Gatekeeper-standardindstillinger.

Programmer fra andre kilder end App Store bliver normalt også signeret med et Apple-udstedt udviklercertifikat. På denne måde kan du validere, at programmet er ægte, og at det ikke er blevet ændret. Programmer, der er udviklet internt, skal også signeres med et Apple-udstedt udvikler-id, så du kan validere deres integritet.

Obligatorisk adgangskontrol (MAC) kræver kodesignering for at aktivere rettigheder, der er beskyttet af systemet. Programmer, som kræver adgang gennem firewallen, skal for eksempel kodesigneres med den passende MAC-rettighed.

Godkendelse og digital signering

macOS indeholder en nøglering og andre værktøjer, som understøtter teknologi til godkendelse og digital signering, såsom smart cards og S/MIME. Tilsammen giver de mulighed for en nem og sikker lagring af brugeroplysningerne og de digitale identiteter.

Nøglering-arkitektur

macOS indeholder en nøgleringsfunktion, som gør det nemt og sikkert at lagre brugernavne og adgangskoder, herunder digitale identiteter, krypteringsnøgler og sikre noter. Du får adgang til funktionen ved at åbne programmet Hovednøglering under /Programmer/Hjælpeprogrammer/. Ved at bruge en nøglering behøver brugeren ikke at indtaste – eller endda huske – brugeroplysningerne til hver eneste ressource. Der bliver lavet en indledende standardnøglering til hver Mac-bruger, selvom brugerne kan lave andre nøgleringe til specifikke formål.

Ud over brugernøgleringe anvender macOS en række nøgleringe på systemniveau, som holder styr på ikke-brugerspecifikke godkendelsesoplysninger, f.eks. netværksoplysninger og PKI-certifikat (Public Key Infrastructure). En af disse

nøgleringe, System Roots, kan ikke ændres og lagrer internet-PKI-rodcertifikat for at understøtte almindelige opgaver såsom online-banktjenester og e-handel. Du kan ligeledes implementere internt tilvejebragte CA-certifikater (certifikatmyndigheder) til administrerede Mac-computere for at hjælpe med at validere interne websites og tjenester.

Framework til sikker godkendelse

Data i nøgleringen partitioneres og beskyttes med adgangskontrollister (ACL'er), så brugeroplysninger lagret af programmer fra tredjeparter ikke kan tilgås af programmer med forskellige identiteter, medmindre brugeren udtrykkeligt godkender dem. Denne beskyttelse leverer mekanismen til at sikre godkendelsesoplysningerne på Apple-enhederne på tværs af en række programmer og tjenester i din virksomhed.

Touch ID

Mac-systemer med en Touch ID-sensor kan låses op ved hjælp af et fingeraftryk. Touch ID afløser ikke behovet for en adgangskode, som stadigvæk er nødvendigt til at logge ind efter start, genstart, eller når brugeren har logget ud af en Mac-computer. Når de er logget ind, kan brugerne hurtigt godkende med et Touch ID, hver gang de bliver bedt om en adgangskode.

Touch ID kan også bruges til at låse op for adgangsbeskyttede noter i programmet Noter, vinduet Adgangskoder i Safari-indstillingerne og mange indstillingsvinduer i Systemindstillinger. For at øge sikkerheden skal brugerne indtaste en adgangskode i stedet for at bruge Touch ID til at låse op for vinduet Sikkerhed & anonymitet i Systemindstillinger. Hvis FileVault er aktiveret, skal brugerne også indtaste en adgangskode for at administrere indstillinger til Brugere & grupper. Flere brugere, som logger ind på den samme Mac-computer, kan bruge Touch ID til at skifte konto.

Få yderligere oplysninger om Touch ID og funktionens sikkerhed i supportartiklen fra Apple "Om avanceret sikkerhedsteknologi for Touch ID" på support.apple.com/HT204587.

Auto-login med Apple Watch

Brugere med Apple Watch kan bruge det til automatisk at låse op for deres Mac. Bluetooth Low Energy (BLE) og "peer-to-peer" Wi-Fi gør det muligt for Apple Watch at låse sikkert op for en Mac-computer efter at have sikret, at enhederne er i nærheden af hinanden. Dette kræver, at en iCloud-konto med totrinsgodkendelse (TFA) er konfigureret.

Få mere at vide om protokollen samt flere oplysninger om funktionerne Kontinuitet og Handoff i vejledningen "iOS-sikkerhed" på www.apple.com/dk/business/docs/iOS_Security_Guide.pdf.

Smart cards

macOS Sierra og nyere har indbygget understøttelse af PIV-kort (Personal Identity Verification). Disse kort anvendes i mange kommercielle og offentlige organisationer til TFA, digital signering og kryptering.

Smart cards indeholder en eller flere digitale identiteter, der har en offentlig og en privat nøgle samt et tilhørende certifikat. Ved at låse op for et smart card med PIN-koden (Personal Identification Number) får brugeren adgang til de private nøgler, som bruges til godkendelse, kryptering og signering. Certifikatet afgør, hvad en nøgle kan bruges til, hvilke attributter der er knyttet til det, og om det er valideret (signeret) af en CA.

Smart cards kan bruges til totrinsgodkendelse. De to trin, der skal bruges til at låse op for et kort, er "noget, du har" (kortet) og "noget, du ved" (PIN-koden). macOS Sierra og nyere har indbygget understøttelse af godkendelse med smart cards i login-vinduet samt klientcertifikatgodkendelse til websites i Safari. Systemet understøtter også Kerberos-godkendelse ved hjælp af nøglepar (PKINIT) til single sign-on på Kerberos-understøttede tjenester.

Få flere oplysninger om smart card-anvendelse med macOS i macOS – Håndbog om implementering på help.apple.com/deployment/macos.

Digital signering og kryptering

I Mail-appen kan brugere sende beskeder, der er digitalt signerede og krypterede. Mail opdager automatisk passende RFC 822-mailadresseemner eller alternative emnenavne, hvor der skelnes mellem store og små bogstaver, på certifikater for digital signering og kryptering på vedhæftede PIV-tokens i kompatible smart cards. Hvis en konfigureret mailkonto stemmer overens med en mailadresse på et certifikat for digital signering eller kryptering på et vedhæftet PIV-token, viser Mail automatisk signeringsknappen på værktøjslinjen i et nyt beskedvindue. Hvis Mail har modtagerens mailkrypteringscertifikat eller kan finde det i Microsoft Exchange Global Address List (GAL), vises der et oplåst symbol i værktøjslinjen for den nye besked. Et låst låsesymbol indikerer, at beskeden vil blive sendt krypteret med modtagerens offentlige nøgle.

S/MIME for hver besked

macOS understøtter S/MIME for hver besked. Det vil sige, at S/MIME-brugere kan vælge som standard altid at signere og kryptere beskeder eller vælge at signere og kryptere individuelle beskeder.

Identiteter, som anvendes med S/MIME, kan leveres til Apple-enheder ved hjælp af en konfigurationsprofil, en MDM-løsning, SCEP-protokollen (Simple Certificate Enrollment Protocol) eller Microsoft Active Directory Certificate Authority.

Netværkssikkerhed

Foruden de indbyggede sikkerhedsfunktioner, Apple bruger til at beskytte data lagret på Mac-computere, er der mange foranstaltninger for netværkssikkerhed, som organisationer kan træffe for at beskytte oplysninger, der sendes til og fra en Mac-computer.

Mobiltelefonbrugere skal kunne få adgang til virksomhedens netværk overalt i verden, så det er vigtigt at sikre, at brugerne er autoriserede, og at deres data er beskyttet under overførslen. macOS anvender – og giver udvikleradgang til – standardnetværksprotokoller for godkendt, autoriseret og krypteret kommunikation. For at opfylde disse sikkerhedsmål integrerer macOS gennemprøvede teknologier og de nyeste standarder for Wi-Fi-datanetværksforbindelser.

TLS

macOS understøtter Transport Layer Security (TLS 1.0, TLS 1.1 og TLS 1.2) og DTLS. Systemet understøtter både AES-128 og AES-256 og foretrækker kodepakker med perfekt forward secrecy. Safari, Kalender, Mail og andre internetprogrammer benytter automatisk denne protokol til at sikre en krypteret kommunikationskanal mellem enheden og netværkstjenesterne.

API'er på højt niveau (f.eks. CFNetwork) gør det nemt for udviklere at indføre TLS i deres programmer, mens API'er på lavt niveau (f.eks. SecureTransport)

giver detaljeret kontrol. CFNetwork tillader ikke SSLv3, og programmer, der bruger WebKit (f.eks. Safari), laver en SSLv3-forbindelse.

Fra og med macOS High Sierra og iOS 11 er SHA-1-certifikater ikke længere tilladt for TLS-forbindelser, medmindre brugeren har godkendt dem. Certifikater med RSA-nøgler på under 2048 bit er heller ikke tilladt. Den symmetriske kodepakke RC4 bruges ikke længere i macOS Sierra og iOS 10. TLS-klienter eller -servere, der er implementeret med SecureTransport-API'er, har ikke RC4-kodepakker aktiveret og kan ikke blive forbundet, når RC4 er den eneste tilgængelige kodepakke. Tjenester eller programmer, der kræver RC4, bør opgraderes til at bruge moderne, sikre kodepakker.

App Transport Security

App Transport Security leverer standardforbindelseskrav, så programmer følger bedste praksis for sikre forbindelser, når API'erne NSURLConnection, CFURL eller NSURLSession anvendes. Som standard begrænser App Transport Security kodevalget til kun at omfatte pakker, der indeholder forward secrecy, nærmere bestemt ECDHE_ECDSA_AES og ECDHE_RSA_AES i GCM- eller CBC-tilstand. Programmer kan deaktivere forward secrecy-kravet pr. domæne, hvor RSA_AES i så fald føjes til sættet af tilgængelige koder.

Servere skal understøtte TLS 1.2 og forward secrecy, og certifikater skal være gyldige og signeret med SHA-256 eller endnu bedre med en minimum 2048 bit RSA-nøgle eller en 256 bit elliptisk kurvenøgle.

Netværksforbindelser, der ikke opfylder disse krav, vil mislykkes, medmindre programmet tilsidesætter App Transport Security. Ugyldige certifikater resulterer altid i hardwarefejl og ingen forbindelse. App Transport Security anvendes automatisk på programmer, der er kompileret til macOS 10.11 eller nyere.

VPN

Sikre netværkstjenester såsom VPN (Virtual Private Networking) kræver typisk minimal indstilling og konfiguration for at fungere med macOS. Mac-computere virker med VPN-servere, der understøtter følgende protokoller og godkendelsesmetoder:

- IKEv2/IPSec med godkendelse gennem shared secret, RSA-certifikater, ECDSA-certifikater, EAP-MSCHAPv2 eller EAP-TLS
- SSL VPN med den passende klientprogram fra App Store
- Cisco IPSec med brugergodkendelse gennem adgangskode, RSA SecurID eller CRYPTOCard og maskingodkendelse gennem shared secret og certifikater
- L2TP/IPSec med brugergodkendelse gennem MS-CHAPV2-adgangskode, RSA SecurID eller CRYPTOCard og maskingodkendelse gennem shared secret

Ud over VPN-løsninger fra tredjeparter understøtter macOS følgende:

- **VPN On Demand** til netværk, der bruger certifikatbaseret godkendelse. IT-politikker specificerer, hvilke domæner der kræver en VPN-forbindelse ved brug af en VPN-konfigurationsprofil.
- **Pr.-app-VPN**, som muliggør meget mere detaljerede VPN-forbindelser. MDM kan angive en forbindelse for hvert administreret program og specifikke domæner i Safari. Det er med til at sikre, at data altid bevæger sig til og fra virksomhedsnetværket – og at det ikke sker for en brugers personlige data.

Wi-Fi

macOS understøtter Wi-Fi-protokoller af branchestandard, bl.a. WPA2 Enterprise, for at give godkendt adgang til trådløse virksomhedsnetværk.

WPA2 Enterprise bruger 128 bit AES-kryptering, som giver brugerne størst mulig sikkerhed for, at deres data er beskyttet, når de sender og modtager data via en Wi-Fi-forbindelse. Med understøttelse af 802.1X kan Mac-computere også integreres i en lang række RADIUS-godkendelsesmiljøer. Metoder til trådløs godkendelse med 802.1X omfatter EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 og LEAP.

WPA/WPA2 Enterprise-godkendelse kan også bruges i login-vinduet af macOS, så brugeren logger ind for at blive godkendt i netværket.

Indstillingsassistenten i macOS understøtter 802.1X-godkendelse med brugernavn og adgangskode ved hjælp af TTLS eller PEAP.

Firewall

macOS indeholder en indbygget firewall, som beskytter Mac-computeren mod angreb ved netværksadgang og denial-of-service-angreb. Systemet understøtter følgende konfigurationer:

- Blokering af alle indgående forbindelser, uafhængigt af program
- Automatisk tilladelse af indbygget software til at modtage indgående forbindelser
- Automatisk tilladelse af downloadet og signeret software til at modtage indgående forbindelser
- Tilføjelse og afvisning af adgang baseret på brugerspecificerede programmer
- Forhindring i, at Mac-computer svarer på ICMP-forespørgsler om probing og portscan

Single sign-on

macOS understøtter godkendelse til virksomhedsnetværk med Kerberos. Programmer kan bruge Kerberos til at godkende brugere i tjenester, de har tilladelse til. Kerberos kan også bruges til en række netværksaktiviteter, fra sikre Safari-sessioner og godkendelse af netværksfilsystem til programmer fra tredjeparter. Certifikatbaseret godkendelse (PKINIT) understøttes, selvom programimplementering af en udvikler-API er påkrævet.

GSS-API SPNEGO-tokens og HTTP Negotiate-protokollen virker med Kerberos-baserede godkendelsesgateways og Windows Integrated Authentication-systemer, der understøtter Kerberos-billetter. Kerberos-understøttelse er baseret på open-source-projektet Heimdal.

Følgende krypteringstyper understøttes:

- AES128-CTS-HMAC-SHA1-96
- AES256-CTS-HMAC-SHA1-96
- DES3-CBC-SHA1
- ARCFOUR-HMAC-MD5

Kerberos konfigureres ved at indhente billetter med Ticket Viewer, logge ind på et Windows Active Directory-domæne eller bruge kommandolinjeværktøjet `kinit`.

AirDrop-sikkerhed

Mac-computere, der understøtter AirDrop, bruger BLE og Apples egen "peer-to-peer" Wi-Fi-teknologi til at sende filer og information til enheder i nærheden, herunder AirDrop-kompatible iOS-enheder med iOS 7 eller nyere. Wi-Fi-radioen bruges til at kommunikere direkte mellem enheder uden brug af en internetforbindelse eller et Wi-Fi-adgangspunkt. Denne forbindelse er krypteret med TLS.

Få yderligere oplysninger om AirDrop, AirDrop-sikkerhed og andre Apple-tjenester i afsnittet "Netværkssikkerhed" i vejledningen "iOS-sikkerhed" på www.apple.com/dk/business/docs/iOS_Security_Guide.pdf.

Kontrol af enheder

macOS understøtter fleksible sikkerhedspolitikker og konfigurationer, der er lette at håndhæve og administrere. Det hjælper virksomheder med at beskytte virksomhedsoplysninger og sikre, at medarbejderne lever op til virksomhedskravene, selv hvis de bruger egne medbragte computere – f.eks. som del af en BYOD-ordning (medbring din egen enhed).

Virksomheder kan bruge ressourcer som adgangsbeskyttelse, konfigurationsprofiler og MDM-løsninger fra tredjeparter til at administrere flåder af enheder og hjælpe med at holde virksomhedsdata sikre, selv når medarbejderne har adgang til disse data på deres personlige Mac-computere.

Beskyttelse med adgangskode

På Mac-computere med Touch ID er den minimale adgangskodelængde på otte tegn. Lange og indviklede adgangskoder anbefales altid, da de er sværere at gætte eller angribe.

Administratorer kan håndhæve indviklede adgangskoder og andre politikker ved hjælp af MDM eller ved at kræve, at brugere installerer konfigurationsprofiler manuelt. En administratoradgangskode er nødvendig for at installere payload til adgangskodepolitik i macOS.

Få detaljerede oplysninger om hver tilgængelig politik i MDM-indstillingerne under help.apple.com/deployment/mdm/#/mdm4D6A472A.

Få udvikleroplysninger om hver politik i dokumentet om konfigurationsprofiler på developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Håndhævelse af konfiguration

En konfigurationsprofil er en XML-fil, der gør det muligt for en administrator at distribuere konfigurationsoplysninger til Mac-computere. Hvis brugeren sletter en konfigurationsprofil, fjernes alle indstillingerne, der er defineret af profilen, også. Administratorer kan håndhæve indstillinger ved at knytte politikker til Wi-Fi og dataadgang. For eksempel kan en konfigurationsprofil, der leverer en mailkonfiguration, også specificere en adgangskodepolitik for enheder. En bruger kan ikke få adgang til mail, medmindre adgangskoden opfylder administratorens krav.

En macOS-konfigurationsprofil indeholder en række indstillinger, der kan specificeres, herunder:

- Politikker for adgangskoder
- Begrænsninger af enhedsfunktioner (f.eks. deaktivering af kameraet)
- Wi-Fi- eller VPN-indstillinger
- Mail- eller Exchange-serverindstillinger
- Indstillinger for LDAP-bibliotekstjeneste
- Firewall-indstillinger
- Brugeroplysninger og nøgler
- Softwareopdateringer

Se en aktuel liste over profiler i dokumentet om konfigurationsprofiler på help.apple.com/deployment/mdm/#/mdm5370d089.

Konfigurationsprofiler kan signeres og krypteres for at validere deres oprindelse, sikre deres integritet og beskytte deres indhold. Konfigurationsprofiler kan også låses til en Mac for helt at forhindre, at de fjernes, eller for at give tilladelse til, at de kun kan fjernes med en adgangskode. Konfigurationsprofiler, der tilmelder en Mac-computer i en MDM-løsning, kan fjernes – men dette fjerner også administrerede konfigurationsoplysninger, -data og -programmer.

Brugere kan installere konfigurationsprofiler, der er downloadet fra Safari, sendt i en mailbesked eller sendt trådløst med en MDM-løsning. Når en bruger konfigurerer en Mac-computer i DEP eller Apple School Manager, downloader og installerer computeren automatisk en profil til MDM-tilmelding.

MDM

Ved hjælp af macOS-understøttelse til MDM kan virksomheder sikkert konfigurere og administrere skalerede Mac-, iPhone-, iPad- og Apple TV-implementeringer overalt i virksomheden. MDM-funktioner er bygget på eksisterende macOS-teknologier såsom konfigurationsprofiler, trådløs tilmelding og Apples tjeneste til push-meddelelser (APNs). APNs bruges for eksempel til at vække enheden, så den kan kommunikere direkte med dens MDM-løsning gennem en sikker forbindelse. Der overføres ingen fortrolige eller navnebeskyttede oplysninger af APNs.

Ved hjælp af MDM kan IT-afdelinger tilmelde Mac-computere i et virksomhedsmiljø, trådløst konfigurere og opdatere indstillinger, overvåge overensstemmelse med virksomhedspolitikker og endda slette eller låse administrerede Mac-computere eksternt.

Tilmelding af enheder

Tilmelding af enheder, en del af Apple School Manager og DEP, er en hurtig, strømlinet metode til at implementere Mac-computere, som en virksomhed har købt direkte fra Apple eller gennem deltagende autoriserede Apple-forhandlere.

Organisationer kan automatisk tilmelde computere i MDM uden fysisk at skulle røre eller forberede computerne, inden brugerne modtager dem. Efter tilmelding logger administratorerne ind på programmets website og forbinder programmet til deres MDM-løsning. De computere, de har købt, kan derefter automatisk tildeles med en MDM-løsning. Når en Mac-computer er blevet tilmeldt, installeres alle MDM-specificerede konfigurationer, begrænsninger eller kontroller automatisk. Al kommunikation mellem computere og Apple-servere krypteres under overførsel med HTTPS (SSL).

Indstillingsprocessen for brugere kan yderligere forenkles ved at fjerne specifikke trin i Indstillingsassistenten, så brugerne kan komme hurtigt i gang. Administratorer kan også styre, hvorvidt en bruger kan fjerne MDM-profilen fra computeren, og sikre, at enhedsbegrænsninger er på plads helt fra starten. Når computeren er blevet pakket ud og aktiveret, tilmeldes den i organisationens MDM-løsning – og alle administrationsindstillinger, programmer og bøger bliver installeret. Bemærk, at tilmelding af enheder ikke er tilgængelig i alle lande eller regioner.

Få yderligere oplysninger relateret til virksomheder i Hjælp til Apples implementeringsordninger på help.apple.com/deployment/business.
Få yderligere oplysninger relateret til uddannelse i Hjælp til Apple School Manager på help.apple.com/schoolmanager.

Begrænsninger

Begrænsninger kan aktiveres – eller i visse tilfælde deaktiveres – af administratorer for at forhindre brugere i at få adgang til et bestemt program, en bestemt tjeneste eller en bestemt funktion på enheden. Begrænsninger sendes til enheder i en payload til begrænsninger i en konfigurationsprofil. Begrænsninger kan anvendes på macOS-, iOS- og tvOS-enheder.

Der kan ses en aktuel liste over tilgængelige begrænsninger for IT-administratorer på: help.apple.com/deployment/mdm/#/mdm2pHf95672

Ekstern sletning og ekstern lås

Mac-computere kan slettes eksternt af en administrator eller bruger. Øjeblikkelig ekstern sletning kan kun lade sig gøre, hvis Mac-computeren har FileVault aktiveret. Når en kommando om ekstern sletning udløses af MDM eller iCloud, sender computeren en anerkendelse og udfører sletningen. Med en ekstern lås kræver MDM, at der anvendes en sekscifret adgangskode på Mac-computeren, hvor alle brugere er låst ude, indtil denne adgangskode bliver indtastet.

Anonymitet

Apple mener, at anonymitet er en grundlæggende menneskeret, og alle Apple-produkter er derfor udformet til at bruge behandling på enheden, hvor det er muligt, begrænse indsamlingen og anvendelsen af data, levere gennemsigtighed og kontrol over dine oplysninger samt at opbygge et stærkt sikkerhedsfundament.

Apple har adskillige indbyggede kontrolfunktioner og muligheder, der gør det muligt for macOS-brugere at beslutte, hvordan og hvornår programmerne anvender deres oplysninger, samt hvilke oplysninger der anvendes. Få flere oplysninger på www.apple.com/dk/privacy.