Säkerhetsfunktioner i macOS

Översikt för IT-personal

Apple har designat macOS-plattformen så att hårdvara, mjukvara och tjänster är integrerade med varandra på ett sätt som bidrar till inbyggd säkerhet och gör plattformen enkel att konfigurera, driftsätta och hantera. macOS innehåller säkerhetsteknik som är avgörande för att IT-personalen ska kunna skydda företagsdata och integrera lösningar i säkra företagsnätverk. Apple har dessutom samarbetat med standardiseringsorgan för att se till att plattformen lever upp till gällande säkerhetscertifieringar. Den här översikten ger kortfattade förklaringar av några av dessa säkerhetsfunktioner.

Dokumentet är indelat i följande ämnesområden:

- **Systemsäkerhet:** Den säkra, integrerade mjukvara som utgör grunden fö macOS.
- **Kryptering och dataskydd:** Den arkitektur och design som skyddar användarens data om enheten tappas bort eller blir stulen.
- **Programsäkerhet:** De system som skyddar Mac från skadeprogram och gör det möjligt att köra program på ett säkert sätt som inte äventyrar plattformens integritet.
- **Autentisering och digital signering:** Funktioner i macOS för hantering av inloggningsuppgifter och stöd för teknik av branschstandard, såsom smarta kort och S/MIME.
- **Nätverkssäkerhet:** Nätverksprotokoll av branschstandard som möjliggör säker autentisering och kryptering vid överföring av data.
- **Enhetskontroller:** Metoder som gör det möjligt att hantera Apple-enheter, förhindra obehörig användning och utföra fjärradering om en enhet skulle tappas bort eller bli stulen.

Mer information om driftsättning och hantering av macOS finns i Referensdokumentet om driftsättning av macOS på help.apple.com/deployment/macos.

Information om säkerhetsfunktioner hos Apple-tjänster som inte tas upp i det här dokumentet finns i handledningen iOS-säkerhet på www.apple.com/se/business/docs/iOS_Security_Guide.pdf.

Systemsäkerhet

Systemsäkerheten i macOS har utformats så att både mjukvara och hårdvara skyddas i alla kärnkomponenter på alla Mac-enheter. Den här arkitekturen är central för säkerheten i macOS och stör aldrig användarupplevelsen.

UNIX

macOS-kärnan utgör operativsystemets hjärta och baseras på BSD (Berkeley Systems Distribution) och Mach-mikrokärnan. BSD ger grundläggande tjänster för filsystem och nätverk, ett schema för identifiering av användare och grupper samt många andra centrala funktioner. BSD begränsar dessutom åtkomsten till filer och systemresurser utifrån användar- och grupp-ID:n.

Mach står för minneshantering, trådkontroll, maskinvaruabstraktion och interprocesskommunikation. Mach-portar representerar åtgärder och andra resurser och ger åtkomst till portarna genom att reglera vilka åtgärder som kan skicka meddelanden till dem. BSD-systemets säkerhetspolicyer och Mach-kärnans funktioner för åtkomstbehörighet utgör grunden för säkerheten i macOS och är direkt avgörande för att säkerställa skydd på lokal nivå.

Kärnans säkerhet är avgörande för säkerheten i hela operativsystemet. Kodsignering skyddar kärnan och kärntillägg från andra tillverkare samt andra systembibliotek och körbara filer som utvecklats av Apple.

Modell för användarbehörighet

En viktig aspekt av Mac-säkerheten är funktionen för att ge och neka åtkomstbehörighet. Behörighet är möjligheten att utföra en viss åtgärd, såsom att hämta data eller köra kod. Behörigheter ges på nivån mappar, undermappar, filer och program samt för specifika data i filer, programfunktioner och administrativa funktioner. Åtkomstbehörighet för program och systemkomponenter kontrolleras med digitala signaturer.

Behörighet kontrolleras på flera nivåer i macOS, såsom Mach- och BSD-komponenterna i kärnan. Behörighet för nätverksprogram kontrolleras med nätverksprotokoll i macOS.

Obligatorisk åtkomstkontroll

macOS använder dessutom obligatorisk åtkomstkontroll, det vill säga policyer för säkerhetsbegränsningar som skapas av utvecklaren och som inte kan åsidosättas. Metoden skiljer sig från diskretionär åtkomstkontroll, som tillåter att användaren åsidosätter säkerhetspolicyer utifrån egna preferenser. Obligatoriska åtkomstkontroller är inte synliga för användaren, utan utgörs av den underliggande teknik som gör det möjligt att erbjuda viktiga funktioner såsom sandlådor, föräldrakontroll, hanterade inställningar, tillägg och System Integrity Protection (SIP).

System Integrity Protection (SIP)

OS X 10.11 och senare innehåller skydd på systemnivå, så kallat System Integrity Protection (SIP), som skrivskyddar komponenter i vissa kritiska områden i filsystemet för att förhindra att de körs eller ändras av skadeprogram. System Integrity Protection är aktiverat som förval vid uppgradering till OS X 10.11. Det är en inställning på den enskilda datorn och om den avaktiveras tas skyddet bort för alla partitioner på den fysiska lagringsenheten. macOS tillämpar den här säkerhetspolicyn på alla processer som körs i systemet, oavsett om de körs i en sandlåda eller med administratörsbehörigheter.

Mer information om dessa skrivskyddade områden i filsystemet finns i Apple Support-artikeln ”Om systemintegritetsskydd på Mac” på support.apple.com/HT204899.

Kärntillägg

macOS har en mekanism för kärntillägg som gör det möjligt att dynamiskt läsa in kod i kärnan utan att användaren behöver omkompilera eller länka om.

Eftersom dessa kärntillägg (KEXT) erbjuder såväl modularitet som dynamisk inläsning utgör de det naturliga alternativet för alla relativt fristående tjänster som kräver åtkomst till interna kärngränssnitt, såsom drivrutiner till hårdvaruenheter och VPN-program.

Kärntillägg som installeras i samband med eller efter installationen av macOS High Sierra måste av säkerhetsskäl godkännas av användaren innan de kan läsas in. Detta kallas användargodkänd inläsning av kärntillägg. Alla användare kan godkänna kärntillägg, inte bara användare med administratörsbehörighet.

I följande fall krävs ingen auktorisering:

- Kärntilläggen installerades före uppgraderingen till macOS High Sierra.
- Kärntilläggen ersätter tidigare godkända tillägg.
- Kärntilläggen kan läsas in utan användargodkännande med kommandot `spctl` som blir tillgängligt vid start från macOS-återställningspartitionen.
- Kärntilläggen kan läsas in via MDM-konfigurationen. I macOS High Sierra 10.13.2 och senare kan du använda MDM för att skapa en lista med kärntillägg som kan läsas in utan användargodkännande. Det här alternativet kräver att Mac-datorn kör macOS High Sierra 10.13.2 som har registrerats i MDM via programmet för enhetsregistrering (DEP) eller via användargodkänd MDM-registrering.

Mer information om kärntillägg finns i Apple Support-artikeln ”Prepare for changes to kernel extensions in macOS High Sierra” på support.apple.com/HT208019.

Lösenord för fast mjukvara

macOS tillåter användning av lösenord för att förhindra oönskade ändringar av inställningarna för den fasta mjukvaran i ett visst system. Lösenordet används för att förhindra följande:

- Start från en obehörig systemvolym
- Ändringar av startprocessen, såsom start i enanvändarläge
- Obehörig åtkomst till macOS-återställningen
- Direct Memory Access (DMA) via gränssnitt såsom Thunderbolt
- Hårddiskläge, vilket kräver DMA

Obs! Apples T2-chip i iMac Pro gör att användare inte kan nollställa lösenordet för fast mjukvara ens om de får fysisk tillgång till Mac-datorn. Säkerhetsåtgärder måste vidtas för att förhindra att användare får fysisk tillgång till innehållet i Mac-datorer som saknar T2-chip.

Internetåterställning

Mac-datorer som inte kan starta från det inbyggda återställningssystemet försöker automatiskt att starta från macOS-återställning via internet. Då visas en snurrande glob i stället för en Apple-logotyp vid start. Vid återställning via internet kan användaren installera om den senaste versionen av macOS eller den version som levererades med den aktuella Mac-datorn.

macOS-uppdateringar distribueras via App Store och genomförs av macOS-installeraren, som med hjälp av kodsignaturer kontrollerar att installeraren och tillhörande paket är äkta innan installationen genomförs. Tjänsten Internetåterställning är dessutom den officiella källan för det operativsystem som levererades med en viss Mac-dator.

Mer information om macOS-återställning finns i Apple Support-artikeln ”Om Återställning för macOS” på support.apple.com/HT201314.

Kryptering och dataskydd

Apples filsystem

Apple File System (APFS) är ett nytt, modernt filsystem för macOS, iOS, tvOS och watchOS. Filsystemet är optimerat för flash-/SSD-lagring och har funktioner såsom stark kryptering, CoW-metadata (Copy on Write), utrymmesdelning, kloning av filer och kataloger, ögonblicksbilder, snabb beräkning av katalogstorlek, atomic safe-save primitives och förbättrade filsystemsgrunder. Dessutom har filsystemet en unik CoW-design som använder I/O-sammanslagning för att öka prestandan och samtidigt säkerställa tillförlitligheten hos data.

APFS allokerar hårddiskutrymme efter behov. När en enskild APFS-behållare har flera volymer delas behållarens lediga utrymme och kan allokeras till vilken som helst av volymerna efter behov. Varje volym upptar bara en del av hela behållaren, så det tillgängliga utrymmet är behållarens totala volym minus den sammanlagda storleken på det utrymme som används av volymerna i behållaren.

I macOS High Sierra måste en APFS-behållare innehålla minst tre volymer, varav de två första är dolda för användaren:

- Förstartsvolym: Innehåller data som behövs för att starta systemvolymerna i behållaren.
- Återställningsvolym: Innehåller återställningsskivan.
- Systemvolym: Innehåller macOS och mappen Användare.

FileVault

På varje Mac finns en inbyggd krypteringsfunktion, FileVault, som skyddar alla lagrade data. FileVault skyddar lagrade data på Mac-datorn med XTS-AES-128-kryptering. Krypteringen kan användas för att skydda hela volymer på interna och externa lagringsenheter. När en användare kör inställningsassistenten och loggar in med Apple-ID och lösenord föreslår assistenten att användaren ska aktivera FileVault och spara återställningsnyckeln i iCloud.

När FileVault aktiveras på en Mac krävs giltiga inloggningsuppgifter innan användaren kan gå vidare med startprocessen och skaffa åtkomst till specialiserade startlägen, såsom Hårddiskläge. Om användaren inte kan ange giltiga inloggningsuppgifter eller en återställningsnyckel förblir hela volymen krypterad och skyddad mot obehörig åtkomst. Det gäller även om den fysiska lagringsenheten tas bort och ansluts till en annan dator.

IT-avdelningar måste definiera policyer för FileVault-konfiguration via MDM och se till att dessa efterlevs för att skydda data i företagsmiljöer. Organisationer kan välja mellan flera alternativ för att hantera krypterade volymer, såsom verksamhetsövergripande återställningsnycklar, personliga återställningsnycklar (som kan deponeras med MDM) eller en kombination av dessa två. Nyckelrotation kan även ställas in som en policy i MDM.

Krypterade skivavbilder

Krypterade skivavbilder i macOS fungerar som säkra behållare där användare kan lagra eller överföra känsliga dokument och andra filer. Krypterade skivavbilder skapas med Skivverktyg som finns i Program > Verktygsprogram. Skivavbilder kan krypteras med 128-bitars eller 256-bitars AES-kryptering. Eftersom en inlänkad skivavbild behandlas som en lokal volym som är ansluten till en Mac, kan användare kopiera, flytta och öppna de filer och mappar som har lagrats där. Innehållet i en skivavbild krypteras och avkrypteras i realtid, precis

som med FileVault. Med krypterade skivavbilder kan användare på ett säkert sätt utväxla dokument, filer och mappar genom att spara en krypterad skivavbild på en extern lagringsenhet, skicka den som en bilaga till ett mejl eller spara den på en fjärrserver.

ISO 27001- och 27018-certifiering

Apple har erhållit ISO 27001- och ISO 27018-certifiering för det informationssäkerhetshanteringssystem (ISMS) som används för infrastruktur, utveckling och drift som berör följande produkter och tjänster: Apple School Manager, iCloud, iMessage, FaceTime, hanterade Apple-ID:n och iTunes U, i enlighet med Statement of Applicability 2.1 från den 11 juli 2017. Apples efterlevnad av ISO-standarden certifierades av British Standards Institution (BSI). ISO 27001- och ISO 27018-certifikaten finns att läsa på BSI:s webbplats:

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

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

Kryptografisk verifiering (FIPS 140-2)

Krypteringsmodulerna i macOS uppfyller den i USA fastställda FIPS-standarden (Federal Information Processing Standards) 140-2 nivå 1 i varje version sedan OS X 10.6. Precis som vid varje stor lansering skickar Apple modulerna till CMVP för verifiering när Mac-operativsystemet lanseras. Detta program säkerställer integriteten hos krypteringsprocesser i Apple-program och tredjepartsprogram som använder krypteringstjänster och godkända algoritmer i macOS på ett korrekt sätt. Alla Apples FIPS 140-2-verifieringscertifikat finns att läsa på CMVP:s webbplats. CMVP har två olika listor med verifieringsstatus för krypteringsmoduler beroende på aktuell status på csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Common Criteria-certifiering (ISO 15408)

Apple har sedan tidigare erhållit macOS-certifiering i enlighet med Common Criteria Certification-programmet och kommer att genomföra en ny utvärdering av macOS High Sierra utifrån Operating System Protection Profile (PP_OSv4.1). Apple arbetar löpande med att utvärdera och eftersträva certifieringar utifrån nya och uppdaterade versioner av cPP-profiler (Collaborative Protection Profiles) som finns idag. Apple spelar en aktiv roll inom International Technical Community (ITC) för att utveckla cPP-profiler med fokus på att utvärdera viktiga mobilsäkerhetstekniker.

Säkerhetscertifieringar, program och handböcker

Apple har i samarbete med myndigheter världen över tagit fram handböcker med anvisningar och rekommendationer för att upprätthålla en säkrare miljö i utsatta miljöer, så kallad ”device hardening”. Handböckerna innehåller definierad och granskad information om hur man konfigurerar och använder de inbyggda funktionerna i macOS för bästa skydd.

Uppdaterad information om säkerhetscertifieringarna av macOS, verifieringar och handböcker finns i Apple Support-artikeln ”Produktcertifieringar, verifieringar och säkerhetsvägledning för macOS” på support.apple.com/HT201159.

Programsäkerhet

macOS innehåller inbyggd teknik som gör att endast betrodda program kan installeras och som skyddar mot skadeprogram. Betrodda program skyddas under körning tack vare säkerhet i flera lager i macOS och programsignering säkerställer att programmen inte kan ändras av någon obehörig.

Gatekeeper

I macOS finns en funktion som heter Gatekeeper och som styr vilka källor som program kan installeras från. Gatekeeper gör att användare och organisationer kan ställa in en lämplig säkerhetsnivå för programinstallation.

Med den högsta Gatekeeper-inställningen kan användare bara installera signerade program från App Store. Med standardinställningen kan användare installera program från App Store samt program signerade med giltigt utvecklar-id. Signaturen talar om att programmet har signerats med ett certifikat utfärdat av Apple och därefter inte har ändrats. Gatekeeper kan vid behov avaktiveras helt med ett Terminal-kommando.

I vissa fall använder Gatekeeper slumpmässiga sökvägar. Det gäller exempelvis när program startas direkt från en osignerad skivavbild eller från den plats där de sparades vid nedladdning och automatiskt avarkiverades. Det här förfarandet gör att programmen placeras på en ospecificerad, skrivskyddad plats i filsystemet innan de startas. Detta förhindrar att program kommer åt kod eller innehåll via relativa sökvägar samt att programmen uppdaterar sig själva om de startas från den skrivskyddade platsen. Användningen av slumpmässiga sökvägar avbryts om ett program flyttas via Finder till exempelvis mappen Program.

Den största fördelen med den här säkerhetsmodellen är att den erbjuder ett brett skydd av ekosystemet. Apple kan snabbt återkalla ett signeringscertifikat om någon obehörig lyckas stjäla eller på annat sätt skaffa tillgång till signering med utvecklar-id och använder det till att sprida skadeprogram. På så sätt kan man stoppa spridningen av skadeprogrammet. Den här typen av skydd undergräver de ekonomiska syftena med attacker med skadeprogram riktade mot Mac och bidrar till ett gott skydd för alla användare.

Användarna kan tillfälligt förbigå de här inställningarna för att installera valfritt program. En organisation kan använda sin MDM-lösning för att göra Gatekeeper-inställningar och se till att de används, samt lägga till certifikat i macOS tillförlitlighetspolicy för utvärdering av kodsignering.

XProtect

macOS innehåller inbyggd teknik för signaturbaserad upptäckt av skadeprogram. Apple arbetar aktivt för att upptäcka nya skadeprogram och virus. Signaturerna i XProtect uppdateras automatiskt och oberoende av systemuppdateringar, allt för att skydda Mac-system mot skadeprogram. XProtect upptäcker och blockerar installationen av kända skadeprogram automatiskt.

Verktyg för borttagning av skadeprogram

macOS innehåller även teknik som åtgärdar problemen om en Mac trots allt skulle drabbas av skadeprogram. Förutom att arbeta för att upptäcka skadeprogram i ekosystemet och på så sätt kunna återkalla utvecklar-id:n (om tillämpligt) samt utfärda XProtect-uppdateringar levererar Apple uppdateringar av macOS för att ta bort skadeprogram från drabbade system som är konfigurerade för att ta emot automatiska säkerhetsuppdateringar.

Verktyget för borttagning av skadeprogram tar emot uppdaterad information och skadeprogrammet tas bort vid nästa omstart. Verktyget för borttagning av skadeprogram gör inte att Mac-datorn startas om automatiskt.

Automatiska säkerhetsuppdateringar

Apple utfärdar uppdateringar av XProtect och verktyget för borttagning av skadeprogram automatiskt. macOS söker automatiskt efter den här typen av uppdateringar varje dag. Mer information om automatiska säkerhetsuppdateringar finns i Apple Support-artikeln ”Mac App Store: Automatiska säkerhetsuppdateringar” på support.apple.com/HT204536.

Säkerhet vid användning

Systemfiler, resurser och operativsystemets kärna är avskärmade från användarens programutrymme. Alla program från App Store körs i en så kallad sandlåda som begränsar åtkomsten till data som har lagrats av andra program. Om ett program från App Store behöver komma åt data från ett annat program måste det använda sig av API:er och tjänster i macOS.

Obligatorisk kodsignering av program

Alla program från App Store har signerats av Apple för att garantera att de inte har manipulerats eller ändrats. Apple signerar alla program som levereras med Apple-enheter. Många av de program som distribueras utanför App Store signeras av utvecklaren med ett Apple-utfärdat utvecklar-id (kombinerat med en personlig nyckel) så att de kan köras med de förvalda Gatekeeper-inställningarna.

Program från andra källor än App Store signeras normalt också med ett Apple-utfärdat utvecklar-id. På så sätt kan användaren validera att programmet är äkta och att ingen har manipulerat det. Program som utvecklas internt bör också signeras med ett Apple-utfärdat utvecklar-id, så att användare kan verifiera deras integritet.

Obligatoriska åtkomstkontroller (MAC) kräver kodsignering för att aktivera rättigheter som skyddas av systemet. Program som kräver åtkomst via brandväggen måste till exempel kodsigneras med rätt MAC-rättighet.

Autentisering och digital signering

macOS innehåller en nyckelringsfunktion och andra verktyg som stöder teknik för autentisering och digital signering, såsom smarta kort och S/MIME. Tillsammans gör de det möjligt att på ett smidig och säkert sätt lagra användarnas inloggningsuppgifter och digitala identiteter.

Nyckelringsarkitektur

macOS innehåller en nyckelringsfunktion, där man på ett smidigt och säkert sätt kan spara användarnamn och lösenord, inklusive digitala identiteter, krypteringsnycklar och säkra anteckningar. Funktionen nås via programmet Nyckelhanterare i Program > Verktygsprogram. Genom att använda en nyckelring behöver användaren inte ange inloggningsuppgifterna för varje resurs eller ens lägga dem på minnet. En första förvald nyckelring skapas för varje Mac-användare, men användarna kan också skapa ytterligare nyckelringar för olika ändamål.

Utöver användarnyckelringar använder macOS ett antal nyckelringar på systemnivå som håller reda på autentiseringsinformation som inte är användarspecifik, såsom nätverksbehörigheter och PKI-certifikat (Public Key

Infrastructure). En av dessa nyckelringar, nyckelringen Systemrötter, kan inte ändras. Den lagrar internet-PKI-rotcertifikat för att underlätta vanliga åtgärder såsom banktjänster och e-handel via internet. Man kan även distribuera interna certifikatutfärdarcertifikat till hanterade Mac-datorer för att underlätta valideringen av interna webbplatser och tjänster.

Säkert autentiseringsramverk

Eftersom data i nyckelringen delas upp och skyddas via behörighetslistor kan inloggningsuppgifter som lagras av tredjepartsappar inte nås av andra program om inte användaren uttryckligen godkänner det. Detta skydd gör det möjligt att skydda autentiseringsuppgifter på Apple-enheter i olika program och tjänster inom organisationen.

Touch ID

Mac-system med Touch ID-sensor kan låsas upp med ett fingeravtryck. Touch ID undanröjer inte behovet av vanliga lösenord, vilka fortfarande krävs vid inloggning efter start, omstart samt när användaren har loggat ut från Mac. När användaren är inloggad kan hen snabbt använda sig av Touch ID överallt där det krävs lösenord.

Touch ID kan även användas till att låsa upp lösenordsskyddade anteckningar i appen Anteckningar, på fliken Lösenord i Safari-inställningarna samt i flera inställningspaneler i Systeminställningar. Av säkerhetsskäl måste användaren dock använda lösenord istället för Touch ID för att låsa upp Säkerhet och integritet i Systeminställningar. Användaren måste även ange sitt lösenord för att hantera användar- och gruppinställningar om FileVault har aktiverats. Om flera användare loggar in på samma Mac kan de använda Touch ID för att växla mellan användarkonton.

Mer information om Touch ID och säkerhet finns i Apple Support-artikeln ”Om avancerad säkerhetsteknik med Touch ID” på support.apple.com/HT204587.

Autoupplåsning med Apple Watch

En användare som har en Apple Watch kan använda den till att automatiskt låsa upp sin Mac. Bluetooth Low Energy-teknik (BLE) och P2P-wifi gör att Apple Watch kan kontrollera att enheterna är i närheten av varandra, för att sedan låsa upp Mac på ett säkert sätt. För att detta ska fungera krävs ett iCloud-konto med tvåfaktorsautentisering aktiverat.

Mer information om protokollet samt om funktionerna Synkad och Handoff finns i handledningen iOS-säkerhet på www.apple.com/se/business/docs/iOS_Security_Guide.pdf.

Smarta kort

macOS Sierra och senare har inbyggt stöd för PIV-kort (Personal Identity Verification). Korten används inom många kommersiella organisationer och myndigheter för tvåfaktorsautentisering, digital signering och kryptering.

Smarta kort innehåller minst en digital identitet med en offentlig och en privat nyckel vardera samt tillhörande certifikat. Genom att låsa upp ett smart kort med PIN-koden får användaren tillgång till de privata nycklar som används för autentisering, kryptering och signering. Certifikatet avgör vad nyckeln kan användas till, vilka attribut som är kopplade till den samt om den är validerad (signerad) av en certifikatutfärdare.

Smarta kort kan användas för tvåfaktorsautentisering. De två faktorer som behövs för att låsa upp ett kort är ”något du har” (kortet) och ”något du

vet” (PIN-koden). macOS Sierra och senare har inbyggt stöd för autentisering med smarta kort i inloggningsfönster samt för klientcertifikatsautentisering till webbplatser i Safari. Det finns även stöd för Kerberos-autentisering med nyckelpar (PKINIT) för enkel inloggning till tjänster som stöder Kerberos.

Mer information om driftsättning av smarta kort med macOS finns i Referensdokumentet om driftsättning av macOS på help.apple.com/deployment/macos.

Digital signering och kryptering

I programmet Mail kan användare skicka digitalt signerade och krypterade meddelanden. Mail upptäcker automatiskt lämpliga RFC822-skiftlägeskänsliga e-postadressämnen eller alternativa ämnesnamn på certifikat för digital signering och kryptering på bifogade PIV-token i kompatibla smarta kort. Signeringsknappen visas automatiskt i verktygsfältet för ett nytt mejl i Mail om ett konfigurerat e-postkonto stämmer överens med en e-postadress på ett certifikat för digital signering eller kryptering på en bifogad PIV-token. En öppen hänglåssymbol visas i verktygsfältet för nytt brev om Mail har mottagarens e-postkrypteringscertifikat eller kan upptäcka det i en global Microsoft Exchange-adresslista. En låst låssymbol innebär att brevet kommer att skickas krypterat med mottagarens publika nyckel.

S/MIME per meddelande

macOS stöder S/MIME per meddelande. Det betyder att S/MIME-användare kan välja att som standard alltid signera och kryptera alla meddelanden eller välja att signera och kryptera enskilda meddelanden.

Identiteter som används med S/MIME kan skickas till Apple-enheter med hjälp av en konfigurationsprofil, en MDM-lösning, SCEP-protokollet (Simple Certificate Enrollment Protocol) eller Microsoft Active Directory Certificate Authority.

Nätverkssäkerhet

Utöver de inbyggda säkerhetsfunktioner som Apple använder till att skydda data som lagrats på Mac-datorer finns det många funktioner och verktyg för nätverkssäkerhet som organisationer kan använda sig av för att skydda information som överförs till och från en Mac.

Mobila användare måste kunna komma åt företagets nätverk i hela världen, men det är samtidigt viktigt att se till att användarna har behörighet och att deras data skyddas under överföringen. macOS använder och ger utvecklare tillgång till standardnätverksprotokoll för autentiserad, auktoriserad och krypterad kommunikation. För att utföra dessa uppgifter på ett säkert sätt använder sig macOS av beprövad teknik och de senaste standarderna för wifi-datanätverk.

TLS

macOS har stöd för Transport Layer Security (TLS 1.0, TLS 1.1 och TLS 1.2) samt DTLS. Det stöder både AES-128 och AES-256 och föredrar kodningsgrupper med PFS (Perfect Forward Secrecy). Safari, Kalender, Mail och andra internetprogram använder protokollet automatiskt för att skapa en krypterad kommunikationskanal mellan enheten och nätverkstjänsterna.

API:er för högnivåfunktioner (såsom CFNetwork) gör det enkelt för utvecklare att använda TLS i sina program, medan API:er för lågnivåfunktioner (såsom SecureTransport) ger en mer finmaskig kontroll. CFNetwork tillåter inte SSLv3-

anslutningar och program som använder WebKit (såsom Safari) kan inte upprätta en SSLv3-anslutning.

Från och med macOS High Sierra och iOS 11 tillåts inte SHA-1-certifikat för TLS-anslutningar som inte först har godkänts av användaren. Certifikat med RSA-nycklar med färre än 2 048 bitar tillåts inte heller. Den symmetriska kodningsgruppen RC4 är märkt för utfasning i macOS Sierra och iOS 10. TLS-klienter och servrar som har implementerats med SecureTransport-API:er har som förval inte RC4-kodningsgrupper aktiverade och kan därför inte ansluta om RC4 är den enda tillgängliga kodningsgruppen. Tjänster och program som kräver RC4 bör uppgraderas för användning med moderna kodningsgrupper så att de blir säkrare.

App Transport Security

App Transport Security tillhandahåller förvalda anslutningskrav så att program följer bästa praxis för säkra anslutningar när API:erna NSURLConnection, CFURL eller NSURLSession används. Som förval begränsar App Transport Security kodvalet till att endast omfatta paket som erbjuder forward secrecy, mer specifikt ECDHE_ECDSA_AES och ECDHE_RSA_AES i GCM- eller CBC-läge. Program kan avaktivera forward secrecy-kravet per domän. I sådana fall läggs RSA_AES till i uppsättningen tillgängliga koder.

Servrarna måste ha stöd för TLS 1.2 och forward secrecy och certifikaten måste vara giltiga och signerade med SHA-256 eller bättre och ha minst en 2 048-bitars RSA-nyckel eller en elliptisk 256-bitars kurvnyckel.

Nätverksanslutningar som inte uppfyller dessa krav kommer att misslyckas, såvida inte programmet åsidosätter App Transport Security. Ogiltiga certifikat leder obevekligen till fel och att ingen anslutning upprättas. App Transport Security används automatiskt i program som kompileras för macOS 10.11 eller senare.

VPN

Säkra nätverkstjänster, såsom VPN (Virtual Private Networking), kräver i regel minimal inställning och konfiguration för att fungera med macOS. Mac-datorer fungerar med VPN-servrar som har stöd för följande protokoll och autentiseringsmetoder:

- IKEv2/IPSec med autentisering med en delad hemlighet, RSA-certifikat, ECDSA-certifikat, EAP-MSCHAPv2 eller EAP-TLS
- SSL-VPN med lämpligt klientprogram från App Store
- Cisco IPSec med användarautentisering via lösenord, RSA SecurID eller CRYPTOCard samt maskinautentisering med delad hemlighet och certifikat
- L2TP/IPSec med användarautentisering via MS-CHAPV2-lösenord, RSA SecurID eller CRYPTOCard samt maskinautentisering med delad hemlighet

Utöver VPN-lösningar från tredje part har macOS stöd för följande:

- **VPN On Demand** för nätverk som använder certifikatbaserad autentisering. IT-policyer anger vilka domäner som kräver en VPN-anslutning genom att använda en konfigurationsprofil.
- **VPN per program**, vilket möjliggör mycket mer detaljkontrollerade VPN-anslutningar. I en MDM-lösning går det att ange en anslutning för varje hanterat program och för specifika domäner i Safari. Detta bidrar till att säkra data alltid skickas till och från företagets nätverk och att användarnas personliga data inte skickas.

Wifi

macOS stöder wifi-protokoll av branschstandard, till exempel WPA2 Enterprise, som ger autentiserad tillgång till trådlösa företagsnätverk. WPA2 Enterprise använder 128-bitars AES-kryptering så att användarna kan känna sig trygga i vetskapen om att deras data förblir skyddade när de skickar och tar emot kommunikation via en wifi-anslutning. Tack vare stöd för 802.1X kan Mac-datorer integreras i en mängd olika RADIUS-autentiseringsmiljöer. Bland de trådlösa autentiseringsmetoder med 802.1X som stöds finns EAP-TLS, EAP-TTLS, EAP-FAST, EAP-AKA, PEAPv0, PEAPv1 och LEAP.

WPA/WPA2 Enterprise-autentisering kan även användas på inloggningsskärmen i macOS, så att användaren loggar in för att autentisera nätverket.

Inställningsassistenten i macOS stöder 802.1X-autentisering med användarnamn och lösenord med TTLS eller PEAP.

Brandvägg

macOS har en inbyggd brandvägg som skyddar Mac mot överbelastnings-attacker och attacker som påverkar nätverksåtkomsten. Den har stöd för följande konfigurationer:

- Blockera alla inkommande anslutningar oberoende av program
- Automatiskt tillåta att inbyggd mjukvara tar emot inkommande anslutningar
- Automatiskt tillåta att nedladdad och signerad mjukvara tar emot inkommande anslutningar
- Lägga till eller neka åtkomst utifrån användarspecificerade program
- Förhindra att Mac-datorn svarar på ICMP-förfrågningar (probing och portscan)

Enkel inloggning

macOS stöder autentisering i företagsnätverk med Kerberos. Program kan använda Kerberos för att autentisera användare för tjänster som de har behörighet till. Kerberos kan även användas vid en rad olika nätverksaktiviteter, från säkra Safari-sessioner och autentisering av nätverksfilsystem till tredjepartsprogram. Certifikatbaserad autentisering (PKINIT) stöds också, men kräver programanpassning av ett utvecklar-API.

GSS-API SPNEGO-tokens och HTTP Negotiate-protokollet används i kombination med Kerberos-baserade nätverksnoder för autentisering och IWA-system (Integrated Windows Authentication) med stöd för Kerberos-biljetter. Kerberos-stödet bygger på projektet Heimdal med öppen källkod.

Följande krypteringstyper stöds:

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

Konfigurera Kerberos genom att inhämta biljetter med Ticket Viewer, logga in på en Windows Active Directory-domän eller använda kommandoradsverktyget `kinit`.

AirDrop-säkerhet

Mac-datorer som stöder AirDrop använder BLE och Apples egen teknik för P2P-wifi vid överföring av filer och information mellan enheter som befinner sig i

närheten av varandra, vilket omfattar AirDrop-kompatibla iOS-enheter med iOS 7 eller senare. Enheterna kommunicerar direkt med varandra genom att sända och ta emot wifi-signaler, utan att gå via internet eller någon wifi-anslutningspunkt. Anslutningen krypteras med TLS.

Mer information om AirDrop, AirDrop-säkerhet och andra Apple-tjänster finns i avsnittet Nätverkssäkerhet i handledningen iOS-säkerhet på www.apple.com/se/business/docs/iOS_Security_Guide.pdf.

Enhetskontroller

macOS har stöd för flexibla säkerhetspolicyer och konfigurationer som är enkla att

genomdriva och hantera. Det hjälper företag och organisationer att skydda information och försäkra sig om att medarbetarna uppfyller företagets krav, även när de använder egna enheter till exempel inom ramen för ett BYOD-program.

Organisationer kan använda resurser som lösenordsskydd, konfigurationsprofiler,

fjärradering och MDM-lösningar från tredje part för att hantera mängder av enheter och skydda företagsdata, även när deras medarbetare använder sina egna Mac-datorer.

Lösenordsskydd

På Mac-datorer med Touch ID måste lösenkoden bestå av minst åtta tecken. Längre och mer komplexa lösenkoder rekommenderas, eftersom de är svårare att gissa eller knäcka.

Administratörer kan se till att alla på företaget använder komplexa lösenord

och andra policyer via MDM eller genom att kräva att användarna installerar konfigurationsprofiler manuellt. Ett administratörslösenord krävs för installation av nyttolast för lösenkodspolicyer i macOS.

Information om de olika policyerna i MDM-inställningarna finns i help.apple.com/deployment/mdm/#/mdm4D6A472A.

Utvecklarinformation om de olika policyerna finns i Configuration Profile Reference på developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef.

Konfigurationskrav

En konfigurationsprofil är en XML-fil som gör det möjligt för administratörer att distribuera konfigurationsinformation till Mac-datorer. Om användaren raderar en konfigurationsprofil försvinner också alla inställningar som definieras av profilen. Administratörer kan genomdriva inställningar genom att knyta policyer till wifi- och dataåtkomst. Exempelvis kan en konfigurationsprofil som tillhandahåller e-postinställningar också ange enhetens lösenordspolicy. Användarens lösenord måste uppfylla administratörens krav för att användaren ska få tillgång till e-posten.

Konfigurationsprofiler i macOS innehåller ett antal möjliga inställningar, däribland:

- Lösenkodspolicyer
- Begränsningar av enhetsfunktioner (exempelvis avaktivering av kameran)
- Wifi- eller VPN-inställningar
- Inställningar av e-postservrar eller Exchange-servrar

- Inställningar för LDAP-katalogtjänster
- Brandväggsinställningar
- Inloggningsuppgifter och nycklar
- Mjukvaruuppdateringar

En aktuell lista med profiler finns i handboken om konfigurationsprofiler på help.apple.com/deployment/mdm/#/mdm5370d089.

Genom att signera och kryptera konfigurationsprofiler kan man verifiera deras ursprung, garantera deras integritet och skydda innehållet. Konfigurationsprofiler kan även låsas till en Mac. På så sätt kan man helt förhindra att de tas bort eller se till att de endast kan tas bort med hjälp av ett lösenord. Konfigurationsprofiler som registrerar en Mac i en MDM-lösning kan tas bort, men detta resulterar att även hanterad konfigurationsinformation, data och program tas bort.

Användare kan installera konfigurationsprofiler som laddas ned från Safari, tas emot i ett e-postmeddelande eller skickas trådlöst via en MDM-lösning. När en Mac registreras i DEP eller Apple School Manager laddas en profil för MDM-registrering ned och installeras automatiskt på datorn.

MDM

macOS har stöd för MDM, vilket innebär att företaget på ett säkert sätt kan konfigurera och hantera skalbara driftsättningar av Mac, iPhone, iPad och Apple TV i hela organisationen. MDM-funktionaliteten bygger på befintliga macOS-tekniker såsom konfigurationsprofiler, trådlös registrering och APNs (Apple Push Notification service). APNs används exempelvis till att väcka enheten så att den kan kommunicera direkt med MDM-lösningen via en säker anslutning. Ingen konfidentiell eller företagsintern information överförs via APNs.

Med hjälp av en MDM-lösning kan IT-avdelningen registrera Mac-datorer i företagsmiljön, konfigurera och uppdatera inställningar trådlöst, övervaka att företagspolicyer efterlevs samt fjärradera och fjärrlåsa hanterade Mac-datorer.

Enhetsregistrering

Enhetsregistrering, som är en del av Apple School Manager och Apples driftsättningsprogram, är ett snabbt och effektivt sätt att driftsätta Mac-datorer som ett företag eller en organisation har köpt direkt från Apple eller från deltagande Apple-auktoriserade återförsäljare.

Organisationer kan automatiskt registrera enheter i MDM utan att hantera enheterna fysiskt eller förbereda dem innan de överlämnas till användarna. Efter registreringen kan administratörer logga in på programmets webbplats och länka programmet till organisationens MDM-lösning. De datorer som organisationen har köpt kan sedan tilldelas automatiskt med en MDM-lösning. När en Mac har registrerats installeras alla MDM-specificerade konfigurationer, begränsningar eller kontroller automatiskt. All kommunikation mellan datorer och Apple-servrar krypteras vid överföringen med HTTPS (SSL).

Man kan förenkla inställningsprocessen för användarna ytterligare genom att ta bort vissa steg i Inställningsassistenten. På så sätt kan användarna börja använda enheterna snabbare. Administratörer kan även styra huruvida en användare ska kunna ta bort MDM-profilen från datorn eller inte och se till att enhetsbegränsningar tillämpas på enheten redan från början. När datorn har packats upp och aktiverats registreras den i organisationens MDM-lösning och alla hanteringsinställningar, program och böcker installeras. Observera att enhetsregistrering inte är tillgängligt i alla länder och områden.

Mer företagsrelaterad information finns i ”Hjälp för Apples driftsättningsprogram” på help.apple.com/deployment/business. Mer utbildningsrelaterad information finns i ”Hjälp för Apple School Manager” på help.apple.com/schoolmanager.

Begränsningar

Begränsningar kan aktiveras (och i vissa fall avaktiveras) av administratörer i syfte att förhindra att användare kommer åt ett program, en tjänst eller en funktion på enheten. Begränsningar skickas till enheter i en nyttolast för begränsningar som bifogas till en konfigurationsprofil. Begränsningar kan tillämpas på macOS-, iOS- och tvOS-enheter.

En aktuell lista med tillgängliga begränsningar för IT-chefer finns här: help.apple.com/deployment/mdm/#/mdm2pHf95672

Fjärradering och fjärrlåsning

Mac-datorer kan fjärraderas av en administratör eller användare. Omedelbar fjärradering kan endast genomföras om FileVault är aktiverat på Mac-datorn. När ett fjärraderingskommando skickas från MDM eller iCloud svarar enheten med en bekräftelse och utför sedan raderingen. Vid fjärrlåsning krävs en sexsiffrig lösenkod, som måste anges för att användaren ska kunna låsa upp Mac-datorn.

Integritet

Apple anser att integritet är en grundläggande mänsklig rättighet. Därför är varje Apple-produkt konstruerad för att bearbeta information internt på enheten i så hög utsträckning som möjligt, begränsa insamling och användning av data, ge användaren insyn och kontroll över sin information och erbjuda en kraftfull säkerhetsgrund.

Apple erbjuder flera inbyggda kontroller och alternativ som gör det möjligt för macOS-användare att själva bestämma när och hur programmen ska använda deras information samt vilken information som ska kunna användas. Mer information finns på www.apple.com/se/privacy.