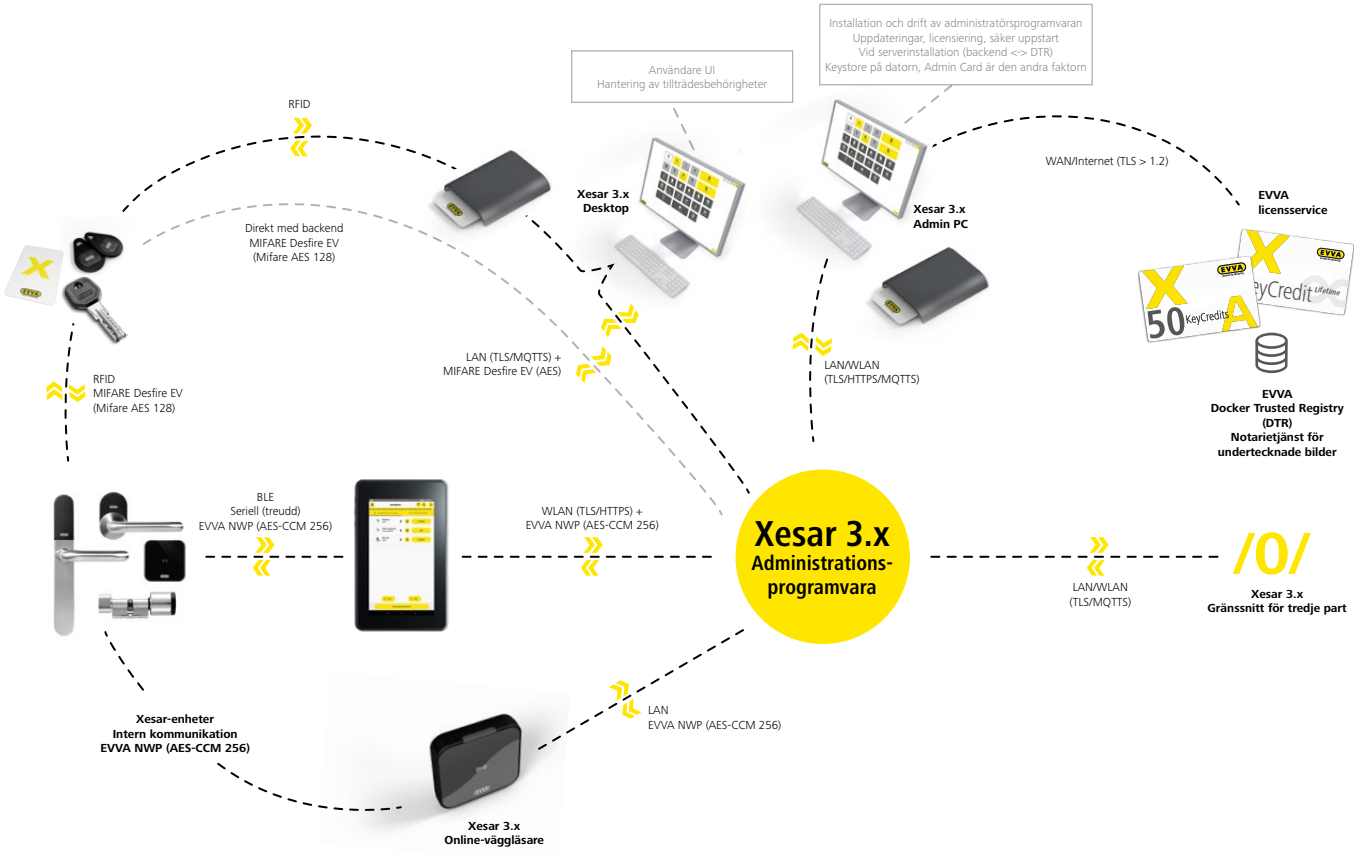
Xesar säkerhetskoncept

Översikt över de viktigaste säkerhetstekniska egenskaperna i ett Xesar-system

Xesar cybersäkerhet



Tillträdesmedier (Xesar 3)

Gränssnitt och kommunikation

För kommunikationen mellan enheter och tillträdesmedier används alltid MIFARE AES-kryptering med 128-bitars AES-kryptering.

- Applikationsnyckeln för tillträdesbehörighet genereras med ett säkert förfarande under Xesar-installationen. Det är en kundhemlighet och EVVA känner inte till den.
- Den lagras endast i krypterad form i säkerhetstjänstens installation.
- Vid tillämpad MIFARE-metod används en session med en egen slumpmässigt genererad nyckel för varje interaktion.

Datalagring

Xesar använder endast säkra tillträdesmedier med skyddad datalagring

- Mifare Desfire EV1 med EAL4+-certifiering eller
- Mifare Desfire EV2/EV3 med EAL5+-certifiering

Säkerhetsinformation

- För att förhindra manipulering bör ett tillträdesmedia endast läggas till i ett Xesar-system för första gången av en behörig användare som använder kodningsstationen på en skyddad plats.
- Construction card är detsamma över hela världen och kan användas överallt för tillträde till Xesar-enheter i fabriksläge. Därför kan ingen tillträdeskontroll utföras med den.
- Ett tillträdesmedia med huvudnyckelbehörighet får endast lämnas ut i undantagsfall och till betrodda personer. Orsak: ett tillträdesmedia med denna behörighetsprofil har
  - obegränsad giltighetstid (max. giltighetstid, se handboken)
  - tillträde till alla tillträdeskomponenter i systemet, även om dessa läggs till/skapas först efter att detta media har utfärdats.

Ett tillträdesmedia med huvudnyckelbehörighet ska förvaras på en säker plats utanför den säkrade anläggningen, så att tillträde till anläggningen är möjligt i nödfall.

Administrationsprogramvara

Leverans

- Alla digitala komponenter i systemet som levereras av EVVA är försedda med en giltig och tidsstämplad kodsignatur.
- Gränssnitt och kommunikation
- All kommunikation med Xesar-administrationen är säkrad med TLS > 1.2, en lista över tillåtna TLS-algoritmer finns på Cipher Suites.
  - För hantering av systemet av flera användare via webbläsare
  - för anslutning av Periphery Manager (fördelad kodningsstation),
  - för interaktion mellan de tjänster som ingår i anläggningen
  - för interaktion med gränssnittet för tredjepartssystem

Autentisering

OWASP-riktlinjerna har följts där detta är meningsfullt.

- Autentiseringen för hantering av anläggningen via webbläsare är lösenordsskyddad:
  - Det första administratörslösenordet genereras slumpmässigt vid installationen (inga standardinställningar)
  - Alla lösenord som skapas måste ha en minimilängd och det finns en kvalitetsindikator (zxcvbn: Low-Budget Password Strength Estimation)
  - Lösenord lagras aldrig i klartext (BCrypt)
  - Misslyckade autentiseringar besvaras medvetet generiskt
- Autentiseringen på servicegränssnitt är certifikatbaserat avbildad med mTLS:
  - För anslutning av Periphery Manager
  - Vid interna anslutningar av tjänster som är beståndsdelar av anläggningen
  - Vid anslutning till gränssnittet för tredjepartssystem via MQTT-Broker; här används dessutom en token för intern auktorisering.

Auktorisering
- I Xesar-administrationen kan användarrättigheter för behörigheter definieras via användargrupper som sedan enkelt kan tilldelas respektive användare
- En användares respektive åtgärder loggas i systemet
- Auktorisering och loggning fungerar även för gränssnittsanvändare

Datalagring
- Alla känsliga uppgifter (t.ex. nyckelmaterial, lösenord) sparas uteslutande i säkerhetstjänsten Installation (Vault) och endast krypterat.
- Vid installationens uppstart "öppnas" Vault för drift via två faktorer (Admin-Card och Admin PC-sparad krypterad nyckelförvaring).
  - Icke-känsliga installations- och konfigurationsdata lagras i en databas som inte är krypterad (se säkerhetsanvisningar).
  - På grund av den arkitekturella utformningen av administrationsprogrammet, där läs- och skrivfunktionerna är åtskilda, sparas alla ändringar som en sekvens av händelser (CQRS-ES) Detta ökar spårbarheten och gör det svårare att manipulera databaserna.

Säkerhetsinformation
- Endast omodifierade produkter från EVVA får användas för installation av systemet. Autenticiteten och integriteten hos alla produkter som EVVA levererar kan verifieras med hjälp av en signatur.
- Kunden ansvarar för säker drift av Xesar administrationsprogramvara;
  - Åtkomst (autentisering och auktorisering) till servermiljön måste säkras så att icke-känsliga installations- och konfigurationsdata inte kan manipuleras på ett enkelt sätt
  - Åtkomst till anläggningens administration ska ske av unikt autentiserade och behöriga användare.
  - De installationskonton som har ställts in ska endast användas under installationen och då endast i undantagsfall (t.ex. återställning av lösenord, återställning).
- Anläggningens säkerhetsdatablad, som genereras för återställningsfall vid installationen, bör endast förvaras i utskriven form på en säker plats (t.ex. kassaskåp).

Information om dataskydd
- När registreringen av personliga åtkomstdata aktiveras bör de landsspecifika dataskyddsbestämmelserna vara kända och följas.
- Automatisk upplösning av kopplingen mellan personer och åtkomstdata kan konfigureras via administrationsprogrammet. Se handboken för information om programvarufunktioner och förfaranden.

Underhållsenhet (Xesar-surfplatta)

Gränssnitt och kommunikation
- För att en ny Xesar-enhet ska kunna läggas till i ett Xesar-system transporteras anläggningsnyckeln krypterad med AEAD-krypteringsmetoden och en 128-bitars AES-nyckel. Denna nyckel härleds från en PIN-kod som en andra faktor – som inte sparas på enheten – med hjälp av en kryptografisk nyckelavledningsfunktion (KDF, AES-CMAC-PRF-128).
- Konfigurationsdata för komponenter i anläggningen transporteras krypterade med AEAD-krypteringsmetoden och den komponentspecifika 256-bitars AES-nyckeln (se även Cybersäkerhet Xesar-enheter).

Säkerhetsinformation
- Den underhållssurfplatta som levereras av EVVA bör endast användas för systemunderhåll.
- Inga andra program bör installeras på den här surfplattan.
- Konfigurationsdata är säkrade med en PIN-kod för installation av nya Xesar-komponenter. Denna ska
  - konfigureras i systeminställningar efter installation i systemet, så att systemet inte använder standardvärdet (dvs. 0000).
  - delas endast med kända och betrodda personer.
- Registrering hos Google krävs inte för användning av Xesar.
- Aktivering av nätverkskommunikation (WLAN) ska endast ske vid behov och ett säkert privat nätverk ska användas (dvs. inte internet)
- Endast systemuppdateringar som rekommenderats och testats av EVVA får installeras.

Enheter

Gränssnitt och kommunikation

- För kommunikationen med enheten används alltid (trådlöst och seriellt) en AEAD-krypteringsmetod med 256-bitars AES-nycklar (AES-CCM).
- Kommunikationsnyckeln genereras specifikt för varje komponent i Xesar-administrationsprogrammet med ett säkert förfarande och är en kundhemlighet som inte är känd för EVVA.
- När komponenterna har installerats i systemet kan endast användaren göra ändringar i komponenternas status eller konfiguration
- Nyckelmaterial kan uppdateras på enheten med motsvarande säkerhet (autentisering, krypterad överföring)
- Brute force-attacker är på grund av nyckelstorleken inte enkla att genomföra med de symmetriska metoderna ens under post-quantum-tiden. Vid batteridrivna enheter kommer försörjningen dessutom endast att möjliggöra en liten andel av de försök som krävs på grund av kombinatoriken, särskilt även på radiosträckan.

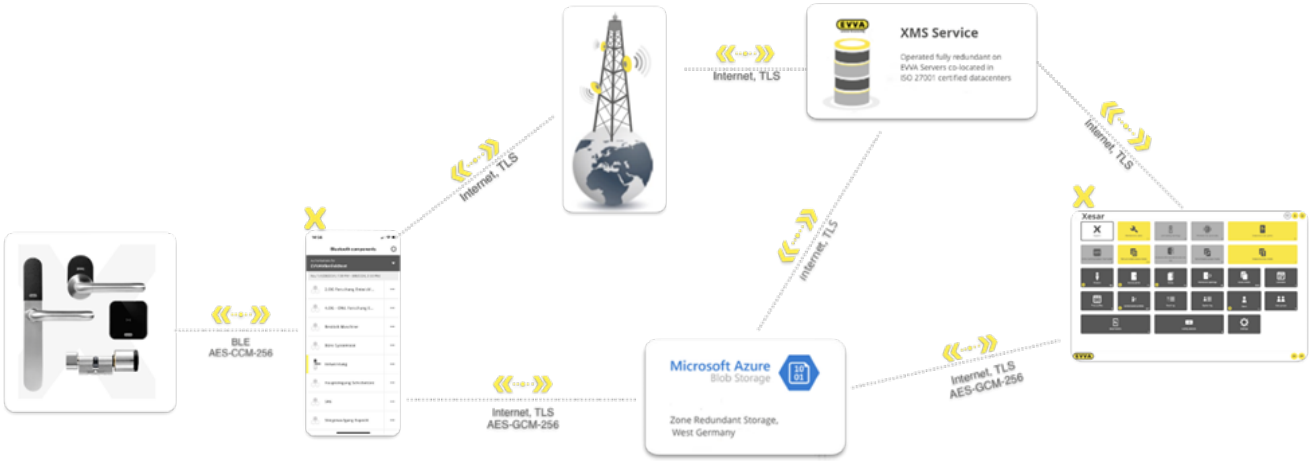
Dataminne

- Nyckelmaterial, känslig konfiguration och applikationskod lagras på respektive mikrostyrenhet (MC) med bästa möjliga MC-säkerhet (NVRAM, internt flashminne)
  - PIC24-serien: Allmänt segmentskydd och kodsegmentskydd (Family Datasheet, 29.4)
  - NRF52: Access port protection controlled by hardware (APPPROTECT)
  - Huset skyddar mot oförstörande åtkomst till MC:erna (se även mekanisk säkerhet för Xesar-komponenter)
- Anläggningsdata lagras på komponenten i ett minne (EEPROM eller flash) och säkras med en kryptografisk metod med en 128-bitars AES-nyckel (AES-CMAC).

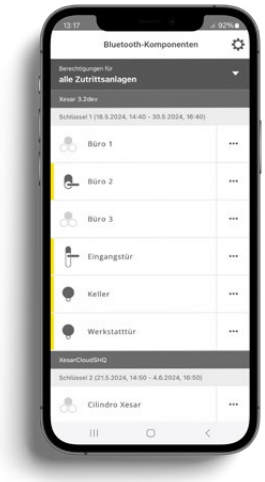
Firmware och uppdatering

- Befintlig firmware laddas från fabrik med en bootloader som inte längre kan ändras och kan uppdateras med motsvarande säkring av bootloadern.
- Firmwarepaket från EVVA signeras med en asymmetrisk metod (RSA-SHA256) och levereras symmetriskt krypterade till Xesar-administrationen. Certifikatkedjan verifieras både i administrationsprogrammet och i underhållsapplikationen.
- För uppdateringen i anläggningen används en AEAD-krypteringsmetod med 256-bitars AES-nycklar (AES-CCM). Firmware-uppdateringsnyckeln genereras specifikt för systemet av Xesar-administrationsprogrammet med ett säkert förfarande och är en kundhemlighet som EVVA inte känner till.
- Endast när den är installerad i systemet kan fler användare utföra en firmware-uppdatering på enheterna.
- För firmware för NRF52 MC:er gäller dessutom:
  - Firmware signeras med en asymmetrisk metod (RSA-SHA256, 2048 bitars nyckel) och verifieras direkt på MC:n.
  - Firmware som är säkrad med en AEAD-krypteringsmetod (AES-CCM) där en 256-bitars AES-nyckel används.
- Firmware för komponenter som införs i ett system uppdateras automatiskt till den senaste kända firmwareversionen för administrationsprogrammet eller underhållsapplikationen.
- Information och kontroll av de uppdateringar som finns tillgängliga från EVVA stöds och möjliggörs av Xesar Installation Manager och Xesar-underhållsprogrammet.

Översikt Mobil Låsning



Xesar-mobilapplikationen (Xesar-app)



Gränssnitt och kommunikation

- All kommunikation med XMS eller molnlagring är TLS-skyddad.
- Alla transaktioner mellan ett Xesar-system och Xesar-appen autentiseras end-to-end med hjälp av ett nyckelutbytesprotokoll (X25519), nyckelavledningsfunktion och meddelandeautentiseringskoder (HKDF-SHA256).
- All kommunikation mellan en Xesar-komponent och mobilapplikationen för överföring av åtkomstdata är uppspelningsskyddad och krypterad inom en session
- Datalagring
- Såvida det stöds av slutenheten lagras känsligt nyckelmaterial på säkra lagringsenheter som tillhandahålls av maskinvaran
  - Android: StrongBox om tillgänglig, tilldelad enheten, molnsäkerhetskopiering inaktiverad av Manifest
  - iOS: CryptoKit nyckelknippa, kan endast användas på enheten, iCloud-synkronisering med provisioneringsprofilen inaktiverad
- All data lagras i en extra krypterad databas på den mobiltelefonen
- Tillträdesdata för ett Xesar-system är redan krypterade av systemet i förväg och kan inte dekrypteras, inspekteras eller manipuleras av mobilapplikationen.
- Säkerhetsinformation
- Mobilapplikationen bör endast laddas ner i sin originalform signerad av EVVA från en officiell butik (dvs. Google Play, Apple App Store)
- EVVA rekommenderar att alla användare av mobilappen
  - använder slutenheter med hårdvarustödda säkerhetsminnen
  - använder minneskryptering
  - säkrar slutenheten med lösenord, PIN-kod eller biometrisk inloggning

Xesar Mobile Support Service (XMS)

Datacenter

- Tjänsten drivs på EVVA-servrar som är placerade i ISO 27001-certifierade, fysiskt åtskilda datacenter i Österrike med hjälp av colocation.
- Alla nödvändiga resurser är redundanta och horisontellt skalbara
- Alla tjänsteslutpunkter är placerade bakom en brandvägg med toppmoderna skyddsmekanismer (IDS, IPS och DoS).

Gränssnitt och kommunikation

- All kommunikation med XMS är säkrad med TLS > 1.2.
  - MQTT Broker (mqtts://mqtt.akx.cloud:443)
    - För lista över tillåtna TLS-certifikat, se MQTT-Broker
  - REST-slutpunkt (https://mss.akx.cloud)

- För autentisering och auktorisering av Xesar administrationsprogramvara
- Lista över tillåtna TLS-algoritmer REST

› XMS fungerar uteslutande som en "relästation" mellan ett Xesar-system och en registrerad smarttelefon med Xesar-appen
  • Alla transaktioner mellan ett Xesar-system och en registrerad smarttelefon med Xesar-appen autentiseras end-to-end med hjälp av ett nyckelutbytesprotokoll (X25519), nyckelavledningsfunktion och meddelandeautentiseringskoder (HKDF-SHA256).
  • Transaktionerna kan därför aldrig initieras eller manipuleras av XMS eller andra Xesar-system.

Datalagring, säkerhetskopiering och nödåterställning

› Endast data som behövs för funktionen sparas
› Data mellanlagras endast under en begränsad tid och i krypterad form för transport mellan Xesar-systemet och en för detta ändamål registrerad smarttelefon med Xesar-appen.
  • Registrering: 48t
  • Uppdatering av behörigheter: 16 dagar
› Åtkomstdata som tillhandahålls av ett Xesar-system krypteras redan före On-Premises-överföringen endast för den registrerade smarttelefonen med Xesar-appen (AES-GCM-256). Dessa data kan inte öppnas av XMS-service, EVVA eller andra Xesar-system.
› Data lagras för närvarande redundant i certifierade molndatacenter i Västtyskland. Arkitekturen är utformad för att kunna utökas till andra regioner/zoner för riktad lagring.
› I händelse av en katastrof som berör en hel zon kan lagringen omdirigeras och uppdateringen av tillträdena göras möjlig igen med hjälp av Xesar-administrationen On-Premises.
› Organisatoriska åtgärder har vidtagits för begränsad och endast auktoriserad åtkomst till lagrade uppgifter
  • Strikt kontrollerade åtkomsträttigheter för operatörer och supportpersonal hos EVVA
  • Strikt hantering av hemligheter för utrullning och drift (SecDevOps)

Övervakning och larm

› Driften av servicekomponenterna övervakas konstant och operatörerna larmas vid avvikelser.
  • De regelverk som upprättats för detta kontrolleras och förbättras kontinuerligt.
› Servicekomponenterna är föremål för kontinuerlig CVE-övervakning och uppdateras i god tid i händelse av hotscenarier.

Information om dataskydd

› Vid utvecklingen har vi arbetat enligt Privacy by Design-principen
› Kunder eller personuppgifter för ett Xesar-system sparas aldrig av XMS
› Data som överförs från ett Xesar-system till en registrerad smarttelefon med Xesar-appen
  • innehåller inga personuppgifter
  • kan eventuellt inte visas av XMS-service, EVVA eller andra Xesar-system
  • Telefonnummer från mobila enheter används uteslutande för samtal till SMS-tjänsteleverantören, men sparas inte av XMS-tjänsten.

Mekaniska säkerhetsegenskaper hos Xesar-enheter

Beslag

Översikt över de mekaniska säkerhetsegenskaperna hos en Xesar dörrbladsläsare.

Godkända certifieringar

› EN 1634-1: 90 minuter
› EN 1634-3
› EN 179
› EN 1906
› med stabilitetsplatta DIN 18 257: ES0
› ÖNORM 3859: 90 minuter

Skydd mot miljöpåverkan

› IP 52 (IP55 med limmad tätning) skydd mot inträngande av skadligt damm och vattenstrålar i monterat tillstånd
› Lackerad elektronik för skydd mot oxidation till följd av kondensvatten
› Användningsförhållanden: -20°C - +55°C
› 3 batterier i säkert utrymme inomhus

Fysikalisk säkerhet

› Multiförskruvning
  • Mekaniskt manipulationsskydd
  • Fritt roterande ytterhandtag

Handtag

Översikt över de mekaniska säkerhetsegenskaperna hos ett Xesar-handtag.

Godkända certifieringar
- EN 1634-1: 90 minuter
- EN 179
- EN 1906
- ÖNORM 3859: 90 minuter
- CE-testad

Skydd mot miljöpåverkan
- Luftfuktighetsintervall: 90% vid 0°C
- Omgivningstemperatur inomhus: +5°C till +50°C
- IP 40

Fysikalisk säkerhet
- Fritt roterande ytterhandtag

Cylinder

Godkända certifieringar
- EN15684 16B30D3D
- SKG***
- SSF3522 för skandinaviska profiler
- EN1634 brandskyddscertifiering (90 min)
- EN179/1125 anti-panik-certifiering
- ÖNORM B 5351:2011 WMZ6-BZ
- CE-certifierad

Skydd mot miljöpåverkan
- IP65-skydd mot inträngande av skadligt damm och kraftig vattenstråle från alla håll i monterat skick.
- Lackerad elektronik för skydd mot oxidation till följd av kondensvatten
- Luftfuktighetsintervall: 90% vid 0°C
- Användningsförhållanden: -20°C - +55°C
- 2 batterier parallellkopplade för högre spänningsstabilitet

Fysikalisk säkerhet
- Fritt roterande ytterknopp
- Borrskydd
- Kärndragningsskydd
- Rotationsdämpning mot angrepp med högfrekvensspindel
- Definierad brottpunkt på yttervredets gänga för att skydda cylinderkärnan mot mekaniska angrepp och förhindra att den demoleras
- Mekaniskt specialverktyg för montering och demontering av cylindervredet

Arkitektonisk säkerhet
- Xesar-cylindern består av ett cylindervred och en cylindermodul som sitter bakom borrskyddet.
- Vred och modul är sammankopplade med kryptografisk säkerhet:
  - Frigivning sker uteslutande inom det mekaniskt ”säkra” området
  - Enkelt byte av vredet förhindrar obehörig åtkomst

Väggläsare (online, offline)

Godkända certifieringar
› CE-certifierad

Skydd mot miljöpåverkan
› Luftfuktighetsintervall 90% vid 0°C
› Omgivningstemperatur -25 °C till +70 °C
› Skyddsklass IP65

Fysikalisk säkerhet
› Äkta glas fram

Arkitektonisk säkerhet
› Xesar väggläsare består av en väggläsarenhet och en styrenhet som befinner sig i ett säkert område.
› Online-väggläsaren består av en väggläsarenhet och en online-styrenhet som befinner sig i ett säkert område.
› Läsenheten och styrenheten är sammankopplade med kryptografisk säkerhet:
  • Frigivning sker uteslutande inom det ”säkra” området
  • Enkelt byte av väggläsaren förhindrar obehörig åtkomst

Andra allmänna säkerhetsfunktioner

Enheter (accesspunkter):
› Tilldelning av accesspunkter till områden och behörighet för områden
› Blacklist för spärrade tillträdesmedia
› Delete-Key– avaktivering av spärrade tillträdesmedia som finns på enhetens blacklist
› Kontorsläge (permanenta öppningar av enheter)
  • Manuell permanent öppning av enheter
  • Automatisk permanent öppning, tidsstyrd mellan två fastställda tidpunkter (start och slut)
  • Automatiskt Office mode avslutas vid fastställda tidpunkter, då även manuellt office mode avslutas (endast avslut)
  • Shop Mode: Office Mode, startas först efter behörigt tillträde
› Händelselogg för tillträdes-, avvisnings- och Office-Mode-händelser
› Tidsbegränsning för tillträdesbehörighet

Tillträdesmedia:
› Virtuellt nätverk möjliggör transport av data via tillträdesmedier resp. användning av dessa av personer i systemet.

Administrationsprogramvara:
› Definierade behörighetsprofiler för användare med olika användarrättigheter (användargrupp)
› Definierade instrumentpanelsvyer för användare efter användarrättigheter (användargrupp)
› Anläggningsstatus på kontrollpanelen
  • Komponenter:
    - Nödvändiga firmware-uppdateringar
    - Nödvändiga konfigurationsuppdateringar
    - Visning av batteristatus
    - Snabb onlinestatus för accesspunkter med EVVA-online-enheter
    - Anslutningsstatus
    - Dörrkontakternas tillstånd
  • Enheter och media:
    - Osäkra accesspunkter
    - Tillträdesmedia som behöver uppdateras
    - Osäkert spärrat media

    Aktiveringar som gjordes med spärrade tillträdesmedia
› Systemlogg för spårbarhet av konfigurationsändringar i administrationsprogramvaran