Forsikring & Pension
September 2017

Suppleringskatalog

Kapitel 2, Appendiks A

Teknisk Specifikation

Elektronisk adgangs-kontrol (ADK)

SikkerhedsBranchen

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf. 41 91 91 91
www.forsikringogpension.dk

Indholdsfortegnelse

A10 Forord

Der findes ikke national lovgivning eller særlige krav til ADK-anlæg, som der f.eks. findes forsikringsselskabskrav til AIA-anlæg. Det bliver dog mere og mere almindeligt, at forsikringsselskaber foreslår eller kræver ADK-anlæg som suppleret sikring.

Denne tekniske specifikation for adgangskontrolanlæg (ADK) giver vejledning til, hvorledes et adgangskontrolanlæg kan beskrives såvel i salgs- og projekteringsfasen som i installations- og overdragelsesfasen, hvorved der tilvejebringes et ensrettet informationsniveau, der giver brugeren et fornuftigt sammenligningsgrundlag.

Den tekniske specifikation er udarbejdet på baggrund af de Europæiske standarder, således at man ved at benytte denne tekniske specifikation følger de overordnede installationsmæssige krav, som er specificeret standarderne.

A11 Indledning

Et adgangskontrolanlæg projekteres og installeres ved, at der pr. adgangspunkt tages stilling til, hvilken klasse (grade) kontrolområdet skal have.

Ud fra kontrolområdets ønskede klasse (grade) skal der træffes beslutning om nedenstående punkter, der alle har betydning for dels valg af udstyr, og dels hvorledes udstyret skal installeres:

- Genkendelsesudstyr på begge sider af adgangspunktet
- Genkendelsesmetode på begge sider af adgangspunktet
- Overvågningsmetode for adgangspunktet
- Forbindelse til overvågningsklient
- Beskyttelse af adgangspunktets udstyr uden for kontrolområdet
- Særlige funktioner

Derudover projekteres og installeres adgangskontrolsystem ved, at der træffes beslutning om en række punkter, der alle har betydning for dels valg af systemets overordnede eller samlede virkemåde, samt dels hvorledes systemet overordnet set skal opbygges og etableres:

- Administration af adgangskontrolsystem
- Transmission af alarmer
- Integration med andre anlæg
- Kortproduktion
- Specialfunktioner
- Operativsystem
- Backup af database

A12 Referencer & Standarder

- DS/EN 60839-11-1:2013 Elektroniske adgangskontrolsystemer – System- og komponentkrav.
- DS/EN 60839-11-2:2015 Elektroniske adgangskontrolanlæg - Anvendelsesvejledning
- EU-Persondataforordningen 2016/679

Den tekniske specifikation for ADK-anlæg gennemgår de vigtigste elementer i standarderne, men ikke nødvendigvis dem alle. Informationerne i specifikationen er i overensstemmelse med standardernes ordlyd, men er der behov for specifikke data, er kendskab til standarderne nødvendig.

Af hensyn til registrering og opbevaring af adgangstransaktioner er kendskab til EU-Persondataforordningen lige så nødvendig.

A13 Definitioner

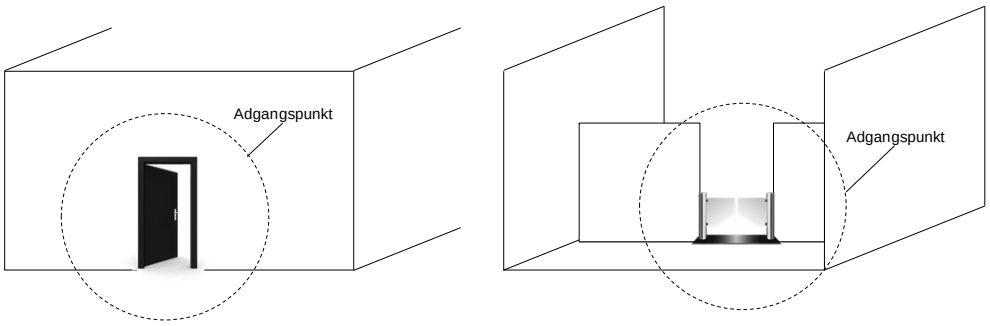
ACU:	Engelsk: Access Control Unit. Dansk: Adgangskontrol-enhed. Samlingspunkt for et adgangspunkts udstyr samt styring og signalbehandling af dette. Eksempelvis samlet i en ADK controller eller distribueret over flere enheder - Se afsnit B30
ADK anlæg:	Et enkeltstående adgangskontrolsystem eller den del af et større adgangskontrolsystem, som er installeret på samme lokation.
Anlægsejer:	Den juridiske person, der har ønsket anlægget etableret, uanset betalingsmåde.
Bruger:	En person, der har adgangsmedie og benytter dette til passage af adgangspunkter.
Controller:	Enkeltstående adgangskontrol-enhed, som er bindeleddet mellem adgangspunktets genkendelsesudstyr, låsemekanisme mm. og adgangskontrolsystemets overvågnings-/betjeningsklient
Dør-overvågning:	Udstyr, der kan overvåge, hvorvidt et lukke (dør mm.) er lukket eller åbent og/eller låst eller oplåst. Eksempelvis en magnetkontakt, micro-switch el. lign.
Kortlæser:	Generel betegnelse for alle typer magnetkortlæsere, RF-læsere, biometriske læsere eller pinkodetastaturer.
Låsemekanisme:	Udstyr, der fastholder en dør, bom, barriere el. lign. position i lukket position. Typisk en el-lås, motorlås eller anden form for elektro-mekanisk pal.
Offline:	Adgangspunkt, der administrativt indgår som en del af et adgangskontrolsystem, men som ikke er permanent tilsluttet systemet.

Online:	Adgangspunkt der er permanent tilsluttet til et adgangskontrolsystem, således at en operatør i realtid kan se status og hændelser for adgangspunktet.
UD-tryk:	Mulighed for manuel åbning af adgangskontrolleret lukke ved f.eks. elektrisk tryk, bevægelsesdetektor, funktion i håndgreb, panikbar, o.l.

A20 Adgangspunkt

Et adgangspunkt er ind-/udgangen til et kontrolleret område, hvor adgangen er begrænset ved hjælp af et lukke.

Typisk er adgangspunktet derfor en dør placeret i åbningen ind til en bygning eller mellem to områder, men et adgangspunkt kan også bestå af eksempelvis en port i et hegn, en barriere i form af en bom, speedgate eller lignende placeret, således at adgangen fra et område til et andet kan kontrolleres.



Adgangspunktet kan adgangskontrolleres ved at lukket er låst ved hjælp af en elektronisk lås, der oplåses, når en person identificerer sig eksempelvis ved en læser ved hjælp af kort, PIN eller biometri eller ved at UD-tryk aktiveres.

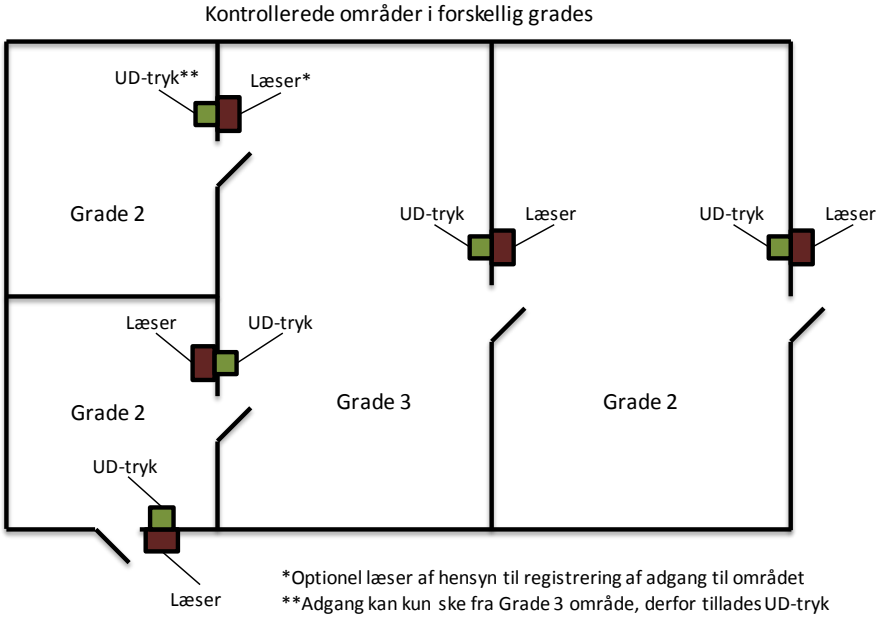
Det kontrollerede områdes klassificering (grade) har betydning for, hvilke krav adgangspunktets skal leve op til i form af bestykning, identifikationsmetode, overvågning mm., således at desto højere grade, desto højere vil kravene være.

I følgende afsnit beskrives de nødvendige installationsmæssige krav, der skal leves op til for, at adgangspunkterne og adgangskontrolsystemet kan leve op til krav, der stilles i de europæiske standarder.

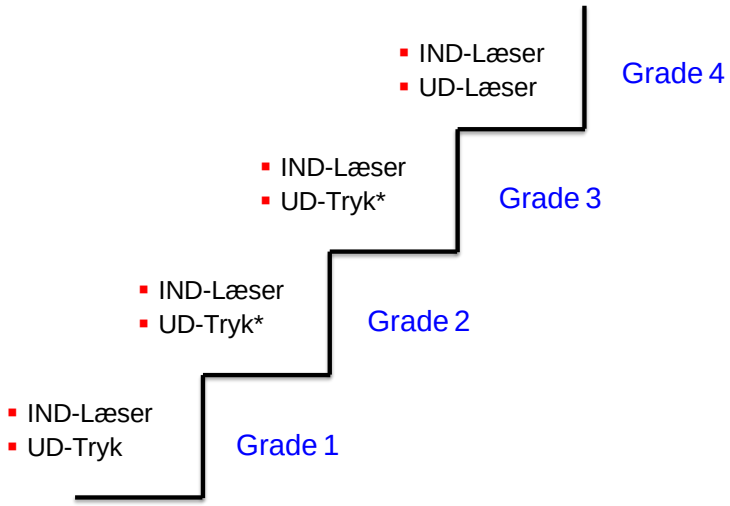
A21 Adgangspunkt genkendelsesudstyr

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning om genkendelsesudstyr (UD-tryk, IND-læser, UD-læser, etc.) på begge sider af adgangspunktet.

- Alle adgangspunkter, der fører til samme kontrollerede område, skal opfylde de samme krav.
- Genkendelsesudstyr og genkendelsesmetode, der giver adgang til et kontrolleret område af højere grade end det område, man kommer fra, skal som udgangspunkt altid leve op til kravene for det højeste område.



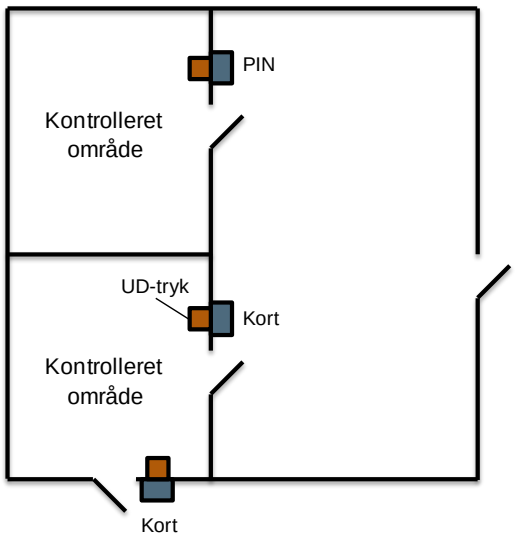
Krav til adgangspunktets genkendelsesudstyr i forhold til det kontrollerede områdes klasse (grade) er, jf. figur nedenfor:



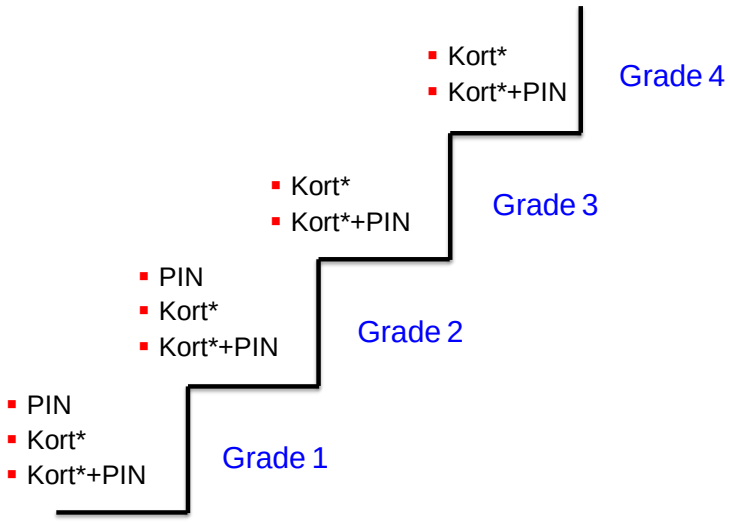
*UD-tryk er tilladt anvendt i Grade 2 og Grade 3, såfremt kunden oplyses, at der er tale om en afvigelse fra kravene i EN 60839-11-1.

A22 Adgangspunkt genkendelsesmetode

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning om genkendelsesmetode (PIN, kort, biometri, etc.) på begge sider af adgangspunktet. Alle adgangspunkter, der fører til samme kontrollerede område, skal opfylde de samme krav.



Krav til adgangspunktets genkendelsesmetode i forhold til det kontrollerede områdes klasse (grade) er, jf. figur nedenfor (hvor der kan vælges mellem de angivne genkendelsesmetoder):

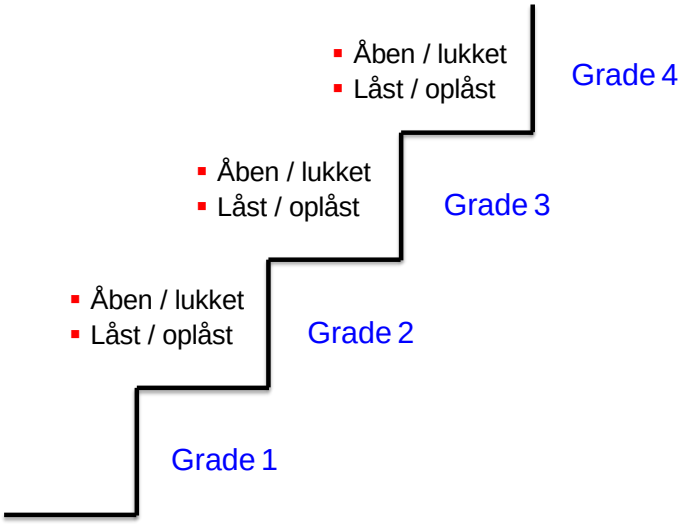


På grade 3 og 4 kan vælges mellem kort eller kort+PIN, men det anbefales her at højne sikkerheden ved at vælge metoden kort+PIN.

*Jf. DS/EN 60839-11-1 standarden skelnes der ikke mellem kort eller biometri.

A23 Adgangspunkt overvågningsmetode

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning om, hvilke overvågningsmetode i forhold til lukkets status, der skal etableres.



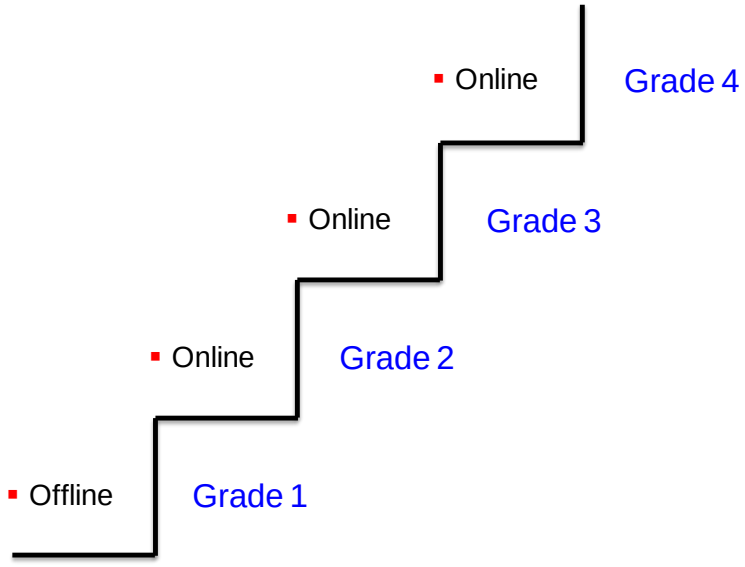
Jf. figur ovenfor er der for Grade 1 ingen krav om overvågning af lukkets status. For Grade 2-4 er der enslydende krav om, at lukket både skal overvåges i forhold til, om det er åbent eller lukket, samt separat om det er låst eller oplåst.

Denne overvågningsmetode giver mulighed for på overvågningsklienten at skelne mellem:

- Normal: Lukket og låst
- Frigivet: Lukket og oplåst
- Åben: Åben og oplåst
- Holdt: Åben efter periode med oplåst
- Forceret/opbrudt: Åben ved tvang

A24 **Adgangspunkt forbindelse**

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning om adgangspunktet skal være forbundet til en overvågningsklient, således at der på denne kan ses alarmer, status, etc.

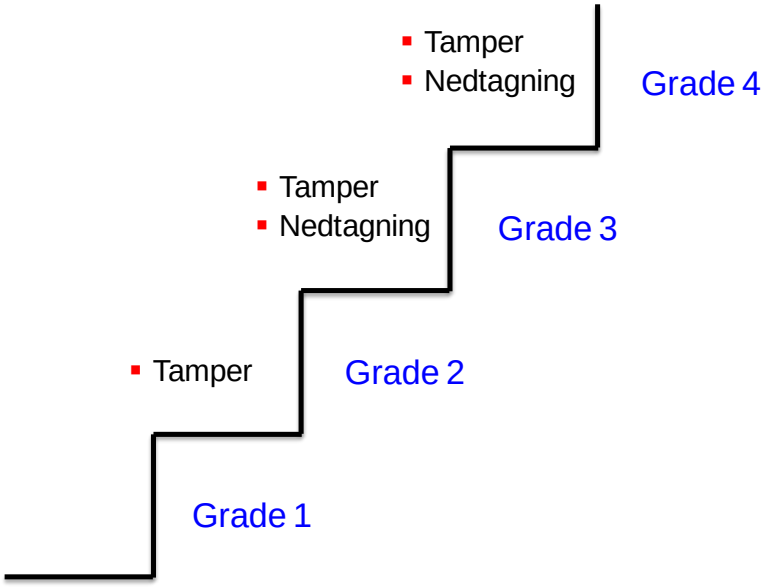


Jf. figur ovenfor er der for Grade 1 ikke krav om, at adgangspunktet skal være forbundet til en overvågningsklient.

For grade 2-4 er der krav om, at adgangspunktet skal være online forbundet til en overvågningsklient, således at detail-krav for disse grades, jf. EN 60839 standarden vedr. visning, alarmering og logning, kan overholdes.

A25 Adgangspunkt beskyttelse

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning, om udstyr monteret uden for det kontrollerede område skal være overvåget mod åbning eller nedtagning.



Jf. figur ovenfor skal udstyr monteret uden for det kontrollerede område (Grade 2-4) have indbygget sabotage/tamper overvågning, således at åbning af udstyret vil medføre alarm.

Jf. figur ovenfor skal udstyr monteret uden for det kontrollerede område (Grade 3-4) have indbygget nedtagnings overvågning, således at nedtagning af udstyret vil medføre alarm.

Kravet til tamper og nedtagningsovervågning er kun gældende, såfremt det er muligt at oplåse adgangspunktet ved manipulation af de interne dele af udstyret.

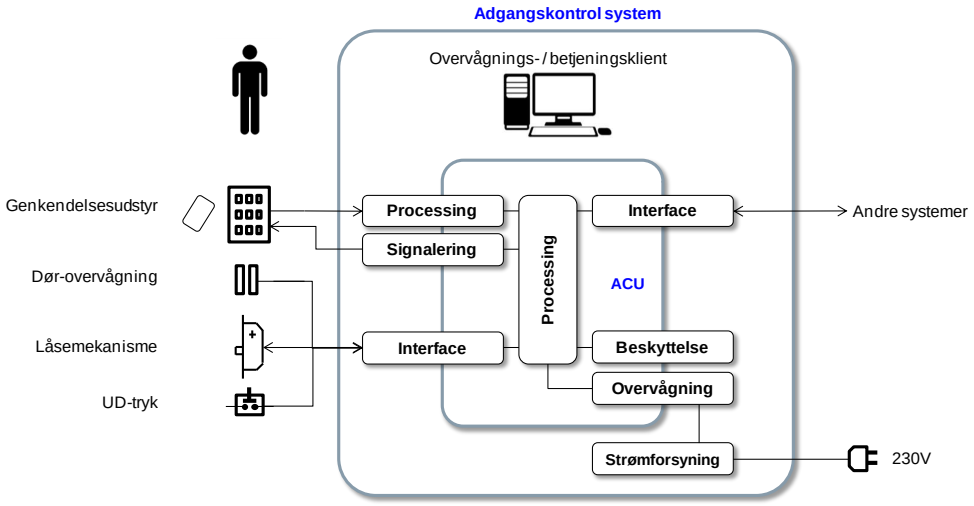
A26 Adgangspunkt særlig funktion

For hvert adgangspunkt ind til et kontrolleret område skal der træffes beslutning om adgangspunktet skal have en eller flere særlige funktioner:

F#	Funktion	Beskrivelse
F1	Video	Adgangen er suppleret med video-overvågning som en del af adgangens dokumentation, sikkerhed eller funktionalitet.
F2	Porttelefon	Opkaldsfunktion fra indgangsdøre. Giver mulighed for fjernoplåsning.
F3	Visitation	Mulighed for stikprøve kontrolfunktion af passerende
F4	Sluse	Parvis sammenkoblede indgangslæsere, hvilket indebærer at en person først kan få adgang gennem den næstfølgende indgangsdør, efter at den først passerede indgangsdør er lukket/låst. Såfremt slusen er forsynet med video, skal åbningen af den følgende slusedør være afhængig af et acceptsignal fra den kontrolperson, der visuelt kontrollerer. Ved etablering af slusefunktion, skal det sikres, at der stadig opretholdes en flugtvej.
F5	AIA-betjening	Giver mulighed for til-/frakobling af AIA-anlægget via kortlæserne.
F6	Antipassback*	Særlig funktion, således at ind-passage for en given person kun tillades, når der forudgående er foretaget udpassage.
F7	Portvagt	Manuel kontrolfunktion af ind-/udpassage.
F8	Etagestyring (elevator)	Læser i elevatorstolen styrer adgangen pr. etage.
F9	ABA styring	Adgangspunktet oplåses ved opstået ABA alarm
F10	Diverse (andet)	Skal beskrives særskilt

*Antipassback er krav ved grade 4, jf. EN-60839-11

A30 Adgangskontrol system



Adgangskontrolsystemer er ofte meget kundespecifikke og findes i mange varianter.

Små adgangskontrolsystemer er oftest enkeltstående anlæg bestående af få adgangspunkter f.eks. en eller flere elektroniske låseenheder med indbygget genkendelsesudstyr (kort læser og/eller PIN-kode tastatur) enten som stand-alone / offline udstyr eller koblet på en enkelt overvågningsklient.

Mellemstore adgangskontrolsystemer er f.eks. flere adgangspunkter med separate kortlæsere, udgangstryk mm. koblet til en eller flere overvågningsklienter via en eller flere separate adgangskontrolenheder (dør-controllere).

Store adgangskontrolsystemer kan bestå af flere separate adgangskontrolanlæg koblet sammen til ét stort system. Hvert separat anlæg vil ofte bestå af mange dør-controllere og adgangspunkter med separate kortlæsere, udgangstryk, mm. evt. suppleret med online eller offline elektroniske låseenheder med indbygget genkendelsesudstyr.

Desto større og mere kompleks et adgangskontrolsystem er, desto større bliver behovet for centraliseret administration/betjening samt lokal eller ekstern overvågning af alarmer og hændelser.

A31 System adgangskontrol software og database

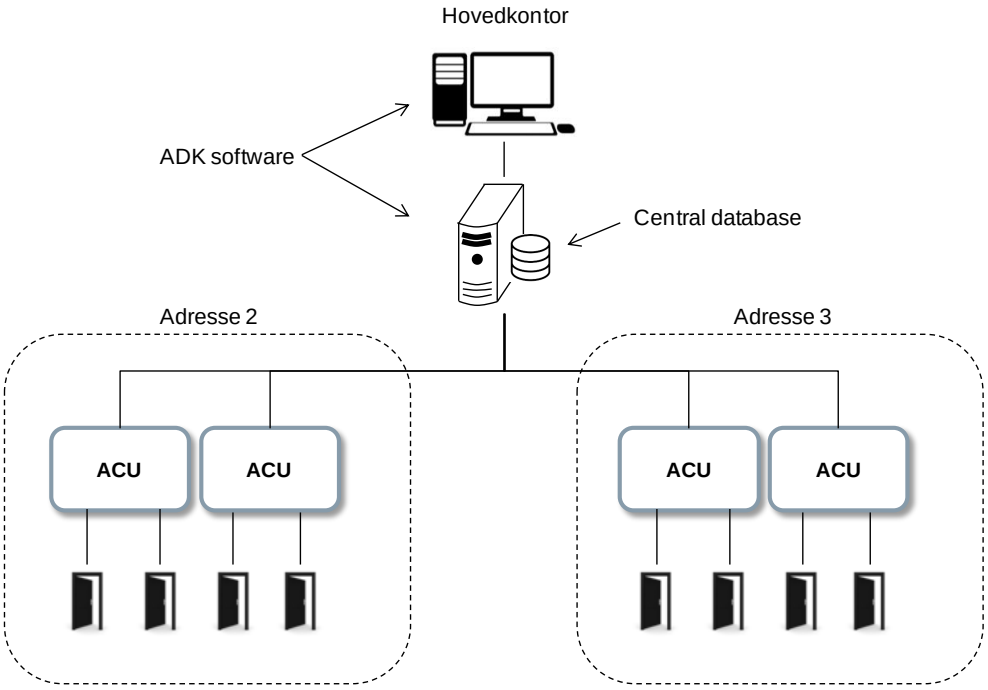
Til overvågning, betjening og/eller konfiguration af et adgangskontrolsystem benyttes typisk en ADK software applikation. I sammenhæng med denne software gemmes data (anlægskonfiguration, loghændelser, brugerdata, mm.) typisk i en database. Ved projektering og installation af adgangskontrolsystemet skal det besluttes, hvilken software og version af denne der skal leveres, og hvor databasen fysisk skal placeres.

System Software

- Software version — En beskrivelse af softwareversion indbefatter angivelse af navn på softwaren samt de aktuelle versions nummer for softwaren.

System Database

- Lokal: — Databasen er fysisk placeret samme sted som adgangskontrolanlægget
- Central: — databasen er fysisk placeret central inden for kundens område/kontrol (f.eks. centralt placeret på virksomhedens hovedkontor)
- Cloud / hosted: — database uden for kundens område/kontrol

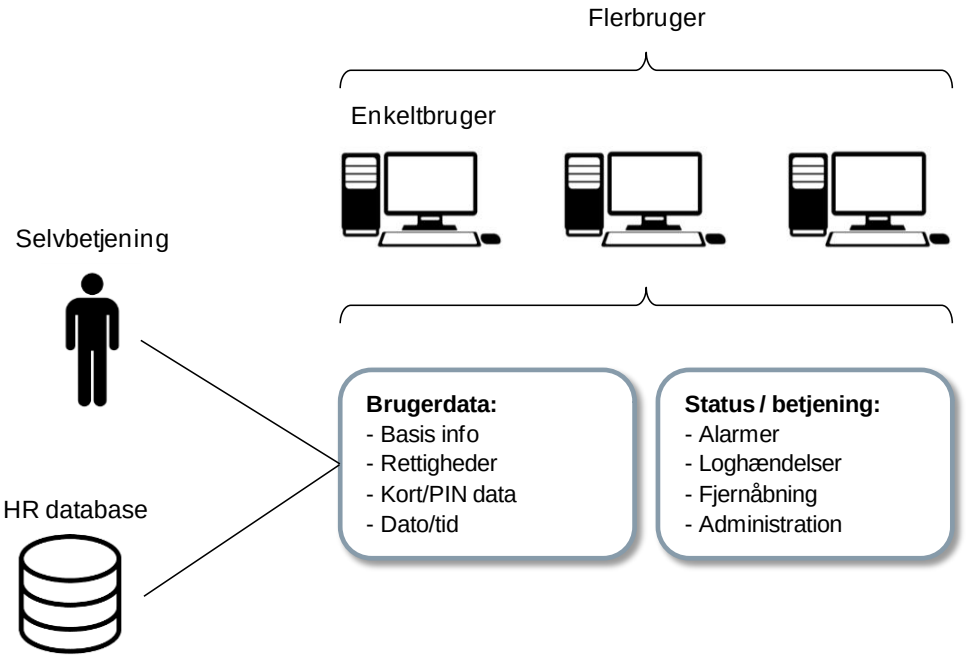


A32 System administration

Administration af et adgangskontrolsystem kan bestå af mange forskellige funktioner, herunder oprette nye brugere, udstede kort, overvåge alarmer, udtrække log-rapporter mm.

I projekterings- og installationsfasen er det derfor vigtigt at beslutte, hvorledes denne administration skal foregå. Til dette er det nødvendigt at skelne mellem, om administration sker på en eller flere af følgende metoder:

- Enkeltbruger: Der etableres én specifik overvågnings-/ betjenings klient.
- Flerbruger: Der etableres et client/server miljø der muliggør overvågning/betjening fra flere klienter.
- Import/export til HR: Administration af brugere/brugerdata sker via dataudveksling med HR system.
- Bruger selvbetjening: Der etableres mulighed for, at brugerne selv kan administrere eller forespørge på rettigheder, brugerdata mm. via selvbetjeningsmulighed.

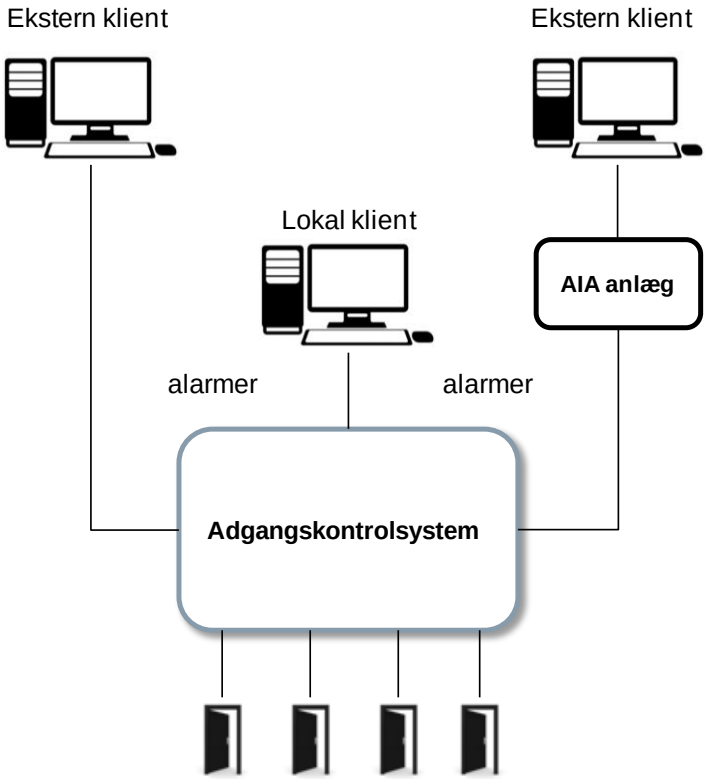


A33 System transmission af alarmer

For at opnå den rette overvågning og reaktion ved alarm fra adgangskontrolsystemet er det vigtigt at beslutte, hvordan alarmer sendes til en overvågningsklient.

Dette kan ske på 3 forskellige måder, enten alene eller i kombination:

- Intern transmission: Alarmer sendes til en lokal overvågningsklient, som er placeret hos kunden.
- Ekstern transmission: Alarmer sendes til en ekstern overvågningsklient, som er placeret på en kontrolcentral / et driftcenter.
- AIA transmission: Alarmer overføres via et AIA anlæg eller via en AIA godkendt transmissionsform.

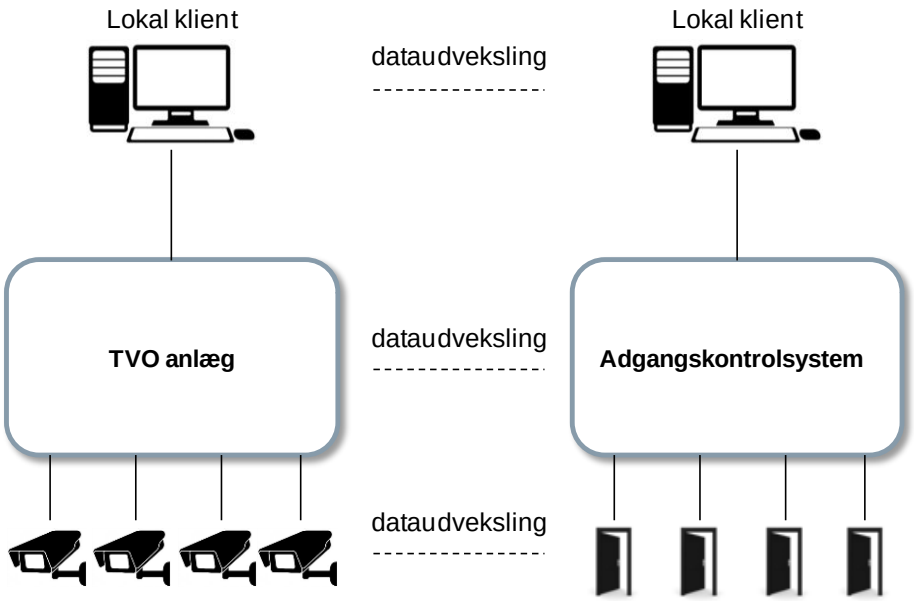


A34 System integration med andre anlæg

Det kan ofte øge værdien og funktionaliteten af adgangskontrolsystemet, hvis der sker dataudveksling mellem adgangskontrolsystemet og andre tekniske anlæg.

- AIA integration: Adgangskontrolanlægget udveksler data med et Automatisk Indbrudsalarm Anlæg eksempelvis med det formål at forhindre adgang til et kontrolleret område, hvor der er aktiv AIA alarmovervågning eller med det formål at til/fra-koble AIA overvåget område fra adgangskontrolanlæggets kortlæsere eller andet genkendelsesudstyr.
- ABA integration: Adgangskontrolanlægget udveksler data med et Automatisk Brandalarm Anlæg eksempelvis med det formål at frigive alle døre ved detekteret brand.
- TVO integration: Adgangskontrolanlægget udveksler data med et TV-overvågningsanlæg eksempelvis med det formål, at kunne verificere personer, der ønsker adgang, eller med det formål at starte optagelser ved alarm fra adgangskontrolanlægget.
- Anden integration: Adgangskontrolanlægget kan udveksle data med andre typer tekniske anlæg med det formål at opnå en forbedret funktion af et eller begge af de anlæg, der integreres.

Integration/dataudveksling kan foregå på flere niveauer: mellem klienter, mellem controllere eller på komponentniveau

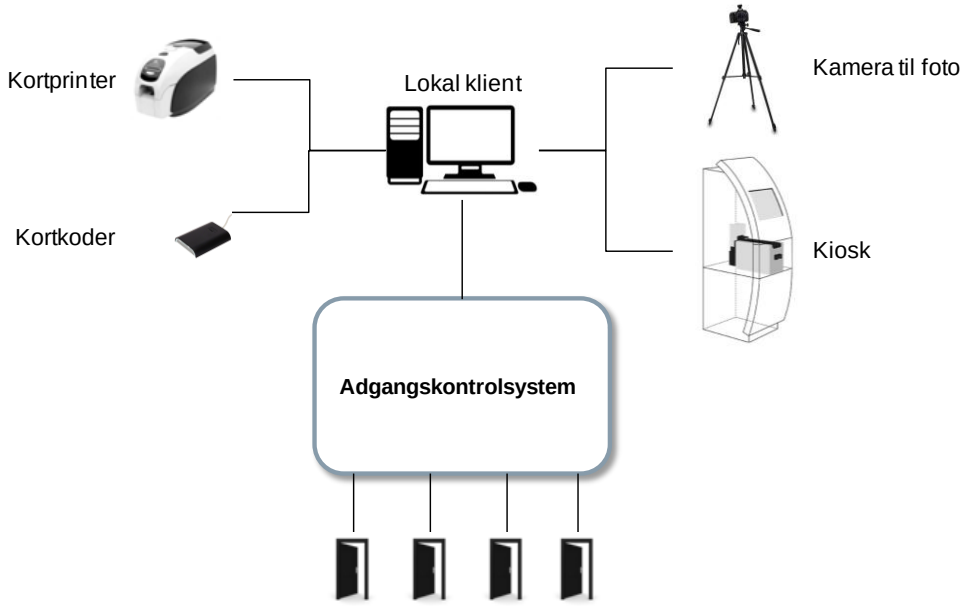


A35 System kortproduktion

Kunder der har behov for et større adgangskontrolanlæg har ofte et ønske behov for selv at kunne producere adgangsmedier i form af kort eller tags eller vil gerne kunne "personalisere" kortene med brugerdata, foto o. lign.
I disse tilfælde kan der etableres forskelligt udstyr som muliggør dette:

- Kortprinter*: Kortprinter er en specialprinter, som er dedikeret til at kunne printe på eksempelvis plastkort.
- Kamera: Er der behov for at kunne tage billede af brugere med henblik på at kunne printe foto på eksempelvis plastkort, kan der tilsluttes et kamera direkte til adgangskontrolanlægget, oftest via overvågnings-/betjeningsklienten.
- Kortkoder*: Kortkoder er udstyr, der er i stand til at programmere kort og/eller tags.
- Andet: Til kortproduktion kan der også leveres andre typer udstyr, eksempelvis lamineringsudstyr, selvbetjeningskiosk etc.

*Der findes kortprintere, som både kan printe og kode kort på samme tid, således at både print og kodning kan ske i én arbejdsgang.



A36 System specialfunktioner

Udover at kontrollere adgangen til områder kan et adgangskontrolanlæg eller dele af det også benyttes til andre formål:

- Betaling med kort: Adgangskontrolanlægget kan benyttes til registrering af betaling, f.eks. kantinebetaling i en virksomhed. Dette kan enten ske ved, at kort har dobbeltfunktion og kan benyttes på både adgangskontrolanlægget og på betalingssystemet. Det kan også ske ved, at der etableres særskilte kortlæsere, som benyttes til registrering af betalinger.
- Gæsteregistrering: Adgangskontrolanlægget kan benyttes til registrering af gæster, enten som en selvbetjeningsløsning eller en administreret løsning, hvor gæster registreres i adgangskontrolsystemet og der eksempelvis udstedes midlertidige adgangskort med ingen eller begrænsede adgangsrettigheder.
- Evakuering: Ved en nødsituation kan adgangskontrolanlægget stille data til rådighed om, hvilke områder der er tomme, eller hvilke områder specifikke personer stadig opholder sig i på trods af ordre om evakuering.
- Andet: Beskrives særskilt.

A37 System backup af database

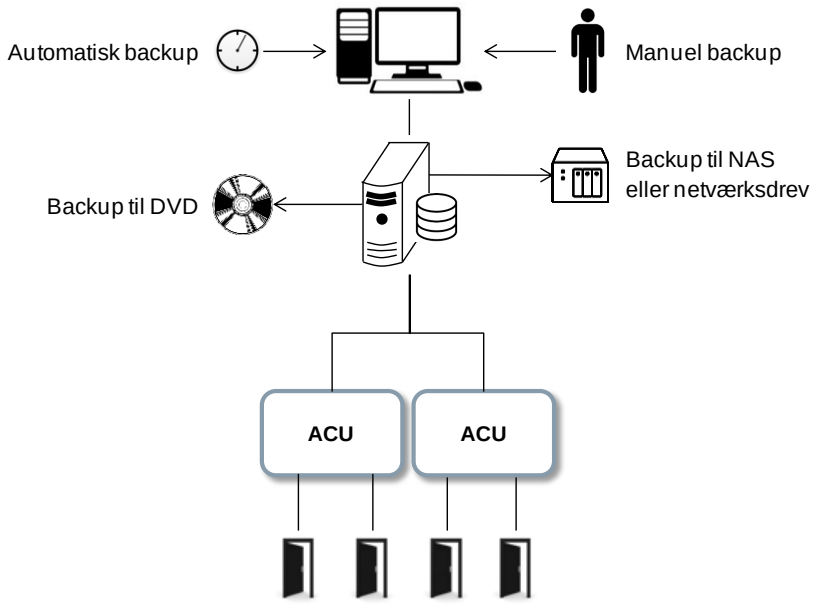
I tilfælde af nedbrud af adgangskontrolanlægget er det vigtigt at have taget backup af adgangskontrolanlæggets database, således at, som minimum, anlægskonfigurationen kan genindlæses.

I forbindelse med backup er det vigtigt at træffe beslutning om, hvor databasen foretages til (netværksdrev, fysisk medie, eller andet), samt hvor tit der skal tages backup, hvem der har ansvaret for udførelsen og/eller kontrol af backup data. Dette bør aftales, før installation igangsættes.

Backup af database kan ske på forskellig måde og til forskellige medier

- Nej: Der er IKKE etableret system, der giver mulighed for løbende backup af adgangskontrolanlæggets database.
- Ja: Der ER etableret system, der giver mulighed for løbende backup af adgangskontrolanlæggets database.
- Manuelt: Backup-systemet kræver en manuel handling før, backup foretages.
- Automatisk: Backup-systemet er etableret således, at backup sker automatisk, typisk med et fastlagt interval imellem hver backup.
- Medie: Backup foretages til medie: DVD, Bånd, lokal sekundær disk, NAS, netværksdrev eller cloud.

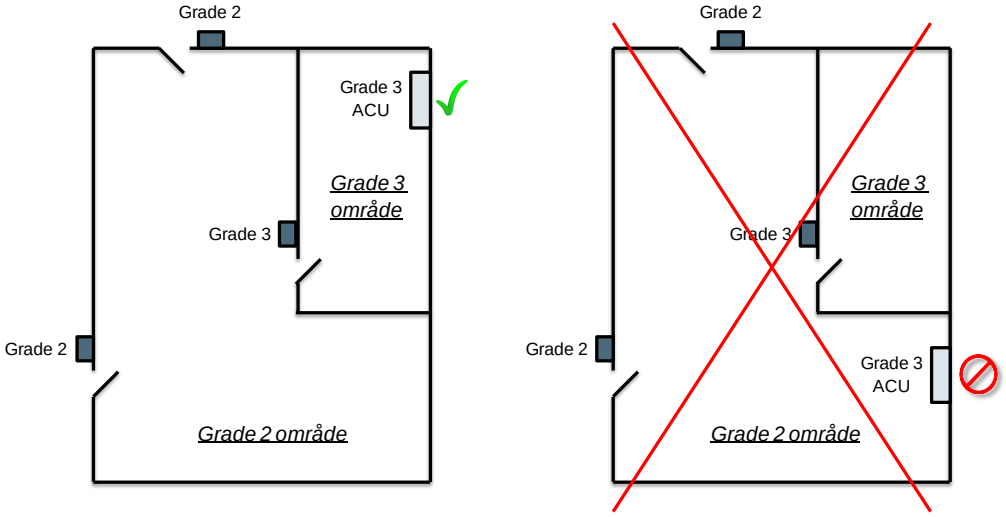
Backup mediet bør aldrig være det samme fysiske medie, som databasen benytter.



A40 Placering af adgangskontrolenheder/ACU

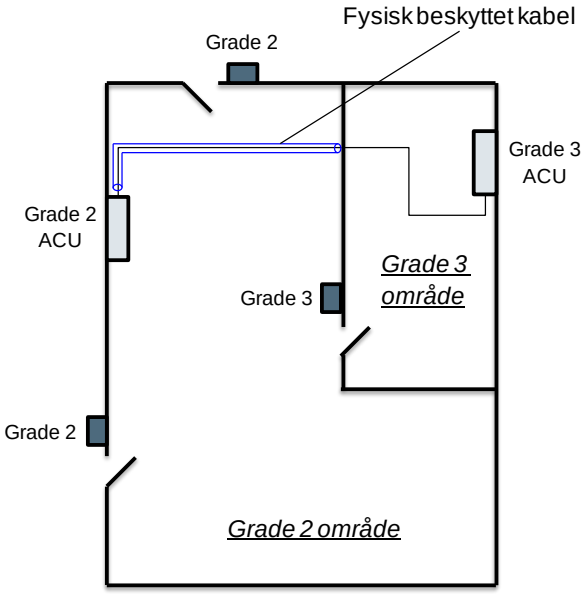
Adgangskontrolenheder (undtagen genkendelsesudstyr), der er kritiske for et områdes sikkerhed, skal altid placeres i et område med samme eller højere grade end det område, der kontrolleres.

Eksempelvis skal en controller, der anvendes til at kontrollere et grade 3 område, altid placeres i et grade 3 område.



A50 Kabler og føringsveje

- Kabler bør altid føres inden for de kontrollerede områder
- Kabler bør altid føres skjult eller være svært tilgængelige
- Kabler, der føres igennem et kontrolleret område af lavere grade, bør altid beskyttes fysisk mod sabotage



A60 Service og vedligehold

Service
Reaktionstiden på serviceanmodninger kan have stor betydning for den sikkerhed, som anlægget er planlagt til at opfylde.

Kunden bør derfor orienteres om konsekvensen for forskellige former for nedbrud og funktionssvigt.

De anbefales at udarbejde en serviceaftale, der specificerer omfanget af serviceforpligtelse, herunder i særdeleshed den nødvendige reaktionstid på serviceanmodninger.

Vedligehold
Adgangskontrolanlæg kræver, som alle andre sikringsanlæg, at der løbende foretages en kontrol af alle anlæggets funktioner.
På adgangskontrolanlæg bør man være særlig opmærksom på betydningen af de mekaniske komponenter på et adgangspunkt.

Det anbefales at udarbejde en vedligeholdelsesaftale, der specificerer omfanget og frekvensen for vedligeholdende eftersyn.

Eftersyn kan blandt andet omfatte:

SYSTEM:
- Kontrol og opdatering af programmering
- Kontrol af utilsigtede forsøg på anvendelse af adgangsmedier
- Kontrol og opdatering af system-backup
- Kontrol af signalforbindelser
- Eventuel opdatering af software

ADGANGSPUNKT:
- Kontrol af elektroniske funktioner
- Kontrol, smøring og justering af alle mekaniske funktioner
- Rengøring af genkendelsesudstyr

INSTALLATION:
- Besigtigelse af synlige installationer
- Udbedring af eventuelle skader.

A70 Supplerende råd og vejledning

Oversigt over DS/EN

Fysiske leverance / installationskrav	Grade					Reference
	0	1	2	3	4	
Indgangskortlæser	Krav	Krav	Krav	Krav	Krav	Table 2 - item 5
Udgangskortlæser	Tilladt	Tilladt	Krav	Krav	Krav	Table 2 - item 6
Udtryk	Tilladt	Tilladt	(Tilladt)	(Tilladt)	Ikke tilladt	Table 2 - item 6
Unik PIN eller kort pr. bruger	Tilladt	Tilladt	Krav	Krav	Krav	Table 4 - item 13
PIN kode alene	Tilladt	Tilladt	Tilladt	Ikke tilladt	Ikke tilladt	Table 4 - item 14
Biometri alene eller sammen med PIN eller kort	Tilladt	Tilladt	Tilladt	Tilladt	Tilladt	Table 4 - item 15
Kort alene	Tilladt	Tilladt	Tilladt	Tilladt	Tilladt	Table 4 - item 16
Kort + PIN	Tilladt	Tilladt	Tilladt	Tilladt	Tilladt	Table 4 - item 17
Overvågning af dør åben / lukket	Tilladt	Tilladt	Krav	Krav	Krav	Table 3 - item 4, 15 & 26 (og 16 & 32)
Overvågning af dør forceret åben / lukket	Tilladt	Tilladt	Krav	Krav	Krav	Table 3 - item 31
Overvågning af dør låst / ikke låst	Tilladt	Tilladt	Krav	Krav	Krav	Table 2 - item 20, Table 3 - item 19
Tamperovervågning (usikret område)	Tilladt	Tilladt	Krav	Krav	Krav	Table 3 - item 30, Table 7 - item 5
Nedtagningskontakt (usikret område)	Tilladt	Tilladt	Tilladt	Krav	Krav	Table 7 - item 6
Overvågnings klient (monitoring Console)	Tilladt	Tilladt	Krav	Krav	Krav	Table 3 - section B
Batteribackuptid (excl. lås og overvågnings klient)				2 timer	4 timer	Table 8 - item 1
Krypteret kommunikation på public netværk	Tilladt	Tilladt	Tilladt	Krav	Krav	Table 7 - item 18
Krypteret kommunikation læser - controller	Tilladt	Tilladt	Tilladt	Krav*	Krav	Table 7 - item 24
Mekanisk beskyttelse af netværk læser - controller	Tilladt	Tilladt	Tilladt	Krav*	Tilladt	Table 7 - item 25

Krav* = den ene af de to krav skal opfyldes