

1 september 2008
Versie 1.0



Certificatieschema
Keurmerk Elektronisch Toegangsbeheer

1 september 2008
Versie 1.0

Certificatieschema

Keurmerk Elektronisch Toegangsbeheer

© SSQ, Stichting Safety, Security and Quality, SSQ 2008

Alle rechten voorbehouden. Alle auteursrechten en databankrechten ten aanzien van deze uitgave worden uitdrukkelijk voorbehouden. Deze rechten berusten bij SSQ.

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, kan voor de aanwezigheid van eventuele (druk)fouten en onvolledigheden niet worden ingestaan en aanvaarden de auteur(s), redacteur(en) e uitgever deswege geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden.

Het gebruik van dit certificatieschema door derden, voor welk doel dan ook is uitsluitend toegestaan nadat een schriftelijke overeenkomst met SSQ is gesloten waarin het gebruiksrecht is geregeld.



Voorwoord

Dit certificatieschema is vastgesteld door het College van Deskundigen 'Elektronisch Toegangsbeheer, waarin de belanghebbende partijen op het gebied van het ontwerp, de installatie, de oplevering en onderhoud van toegangscontrolesystemen zijn vertegenwoordigd. Dit college begeleidt ook de uitvoering van certificatie en stelt zo nodig dit certificatieschema bij. Waar in dit certificatieschema sprake is van "College van Deskundigen" is daarmee bovengenoemd college bedoeld.

Certificaat voor de eindgebruiker

Dit certificatieschema omvat alle eisen waaraan een modern elektronisch toegangscontrolesysteem kan voldoen en maakt het mogelijk om de eindgebruiker (klant) bij oplevering van het toegangscontrolesysteem het certificaat te overhandigen waarin de eisen en afspraken staan bevestigd.

Beheer

Het dagelijks gebruik en beheer van het toegangscontrolesysteem valt onder de verantwoordelijkheid van de eigenaar van het toegangscontrolesysteem. Wel wordt het correct gebruik en beheer als belangrijk beschouwd.

Voor het beheer van het toegangscontrolesysteem zal bij de klant een 'Opgeleid Persoon' (OP) aanwezig moeten zijn die het toegangscontrolesysteem in beheer heeft en aan wie het Technisch toegangscontrolebedrijf de installatie oplevert na installatiewerkzaamheden. De OP-er mag als derde partij zijn georganiseerd buiten de eigenaar om.

Ontwerptraject met PvE (Programma van Eisen)

In het voortraject wordt in overleg met de afnemer de eisen vastgelegd in een Programma van Eisen (PvE). Om een zo volledig mogelijk pakket aan uitgangspunten en criteria met de afnemer op locatie te beoordelen is een universele aanpak vastgelegd in een 'standaard PvE'. De projectie en installatie van het toegangscontrolesysteem zal op basis van dit PvE worden uitgewerkt. Aanvullende eisen kunnen altijd worden toegevoegd aan het PvE.

Elektronische Toegangscontrolesystemen met een centrale verwerkingseenheid.

De toegangscontrolesystemen zoals beschreven in dit certificatieschema sluiten aan bij de functionele eisen die zijn vastgesteld in de NEN 50133-1.

Deze systemen kenmerken zich door een 'centrale verwerkingseenheid' (apparatuur) die het mogelijk maakt de doorgangen te beheren met behulp van (programmeerbare) elektronica. De centrale verwerkingseenheid verzorgt de sturingen voor het ontgrendelen.

Beveiligingsniveau (risicoklasse)

Indien er voor een terrein of object een bepaald beveiligingsniveau is vastgesteld; bijvoorbeeld overeenkomstig de risicoklasse indeling vanuit het Handboek Beveiligingstechniek, dan zal het toegangscontrolesysteem geen nadelige invloed hebben op de bouwkundige, organisatorische en elektronische maatregelen in die bewuste klasse.

Indien de componenten van het toegangscontrolesysteem buiten het beveiligde gebied zijn gemonteerd zal sabotage moeten worden gemeld. In geen geval mogen de doorgangen (deuren) worden ontgrendeld.

Toegangscontrole is geen inbraakbeveiliging

Een toegangscontrolesysteem heeft een andere functie dan een inbraakalarmsysteem. Het beheer van toegangsrechten en het beveiligingsniveau ervan hangt vaak wel af van het risicoprofiel van een object. Afstemming van de specifieke organisatorische maatregelen van het toegangsbeheer met de maatregelen van de inbraakbeveiliging is een noodzaak en dient vooraf met de eindgebruiker te worden uitgevoerd.



Bouwbesluit

Eisen die in het Bouwbesluit worden opgelegd aan deuren en doorgangen gelden ook voor deuren en doorgangen die onderdeel zijn van het toegangscontrolesysteem. De eisen kunnen conflicteren en er zal per installatie moeten worden vastgesteld welke eisen voorrang krijgen. Denk hierbij vooral aan de eisen ten aanzien van brandveiligheid, vluchtwegen, nooduitgangen en inbraakwerendheid.

In hoofdstuk 1 van dit certificatieschema wordt de koppeling met regelgeving gegeven ten aanzien van toegangscontrolesystemen. Als er verwezen wordt naar bijlagen vanuit deze paragraaf zal dat zijn naar een informatief tekstdeel waarin suggesties worden gedaan voor het oplossen van problemen met de vaak tegengestelde eisen rond doorgangen. Dit richt zich met name op vluchtveiligheid, inbraakwerendheid en maatregelen tegen ongewenst gebruik.



Inhoud

	Inhoud	5
1	Inleiding	8
1.1	Algemeen	8
1.2	Toepassingsgebied	8
1.3	Begrippen en afkortingen	8
1.4	Classificatie componenten	10
1.5	Toegangscontrolegebied (zoning)	10
1.6	Koppeling met de regelgeving	10
1.7	Procescertificaat voor de certificaathouder	10
1.8	Keurmerk	10
1.9	Keurmerk op eindresultaat	10
2	Componenten Toegangscontrole	11
2.1	Algemeen	11
2.2	Functionele eisen toegangscontrolesysteem NEN-EN 50133-1	11
2.3	Componenten	11
2.3.1	Sturingen aan elektrische vergrendelingen	12
2.4	Classificatie	12
2.5	Controle op de eisen t.a.v. componenten	12
2.6	Controle op de waarborg en leveringsomvang van de integrale productsamenstelling.	12
2.7	Keurmerk op eindresultaat	13
3	Eisen aan het PvE en de projectie	14
3.1	Algemeen	14
3.1.1	Kwalificaties	14
3.1.2	Eisen samenwerking met de opdrachtgever (PvE)	14
3.1.3	Eisen aan het transmissiesysteem	14
3.1.4	Eisen aan opgeslagen gegevens	14
3.1.5	Zelfstandig functionerende toegangscontrolesystemen	15
3.1.6	Vaststellen PvE	15
3.2	Projectie	15
3.2.1	Vaststellen projectering	16
3.3	Keurmerk op eindresultaat	16
4	Eisen aan het detailontwerp, installeren en opleveren	17
4.1	Algemeen	17
4.2	Kwalificaties	17
4.3	Opstellen detailontwerp	17



4.4	Controle voor uitvoering	17
4.4.1	Controle eisen integraal werkende productsamenstelling	17
4.4.2	Controle vastgesteld PvE en projectering	17
4.4.3	Controle elektrische vergrendelingen	17
4.5	Uitvoering	17
4.6	Controle op uitvoering	18
4.6.1	Controle werking doorgangen	18
4.6.2	Controle op de eisen van het transmissiesysteem	18
4.6.3	Controle op de eisen aan opgeslagen gegevens	19
4.6.4	Controle wijzigingen overzichtstekening	19
4.6.5	Controle op overige eisen	19
4.7	Inbedrijfstelling en opleveren	19
4.8	Oplevercertificaat Toegangscontrolesystemen	19
4.9	Keurmerk op eindresultaat	20
5	Eisen aan het onderhouden	21
5.1	Algemeen	21
5.2	Kwalificaties	21
5.3	Onderhoud	21
5.4	Onderhoudsrapport na onderhoud	21
5.5	Keurmerk op eindresultaat	22
6	Eisen aan het kwaliteitssysteem	23
6.1	Algemeen	23
6.2	Borging eisen uit dit beoordelingsschema	23
6.3	Beheerder van het kwaliteitssysteem	24
6.4	Taken, verantwoordelijkheden en bevoegdheden	24
6.5	Procedures en werkinstructies	24
6.6	Opdrachtvorming	24
6.6.1	Extra eis opdrachtvorming voor het Technisch Toegangscontrolebedrijf	24
6.7	Vakbekwaamheid en Kwalificaties	24
6.7.1	Instantie die examens afneemt	24
6.7.2	Projecteringsdeskundige Toegangscontrolesystemen	25
6.7.3	MBV'er	25
6.7.4	TBV'er	25
6.8	Integriteit personeel – ter informatie	25
6.9	Uitbesteden van werk en inhuur van personeel	25
6.10	Documentenbeheer	26
6.11	Klachten en corrigerende maatregelen – niet zijnde storingen	26
6.12	Archivering	26
6.13	Melden projecten aan de CI – Alleen voor het installatiebedrijf	26
7	Afspraken over de uitvoering van certificatie	27



7.1	Algemeen	27
7.2	Initieel certificatieonderzoek - samenvatting	27
7.3	Opvolgingsaudit – samenvatting	27
7.4	Certificatiepersoneel	28
7.5	Corrigerende maatregelen	28
7.6	Rapportage aan College van Deskundigen	28
8	Lijst van vermelde documenten	29
8.1	Normatieve documenten:	29
8.2	Informatieve documenten	29

Bijlagen

I	Inbraakwerendheid	30
II	Vluchtveiligheid	32
III	Brandveiligheid	33
IV	Modeltekst procescertificaat	34
V	Oplevercertificaat Toegangscontrolesysteem	35
VI	Melden projecten	36
VII	Checklist Opleveren Toegangscontrolesysteem	37
VIII	Standaard PvE Toegangscontrolesysteem	38
IX	Beveiligingsprotocol transmissie	43
X	Classificatie	48
XI	Zonering Toegangscontrolegebied	51
XII	Onderhoudsrapport	52
XIII	Specificatieblad geïntegreerde productsamenstelling	53



1 Inleiding

1.1 Algemeen

Het certificatieschema geeft in de keten de relatie én samenhang aan tussen de producten en de processen om te komen tot een toegangscontrolesysteem dat correct functioneert. De volgende schakels zijn van belang binnen deze keten:

- Producten;
- Programma van Eisen (PvE);
- Projecteren;
- Detailontwerp;
- Installeren;
- Opleveren;
- Onderhoud.

1.2 Toepassingsgebied

Het toepassingsgebied betreft het ontwerpen, installeren, opleveren en onderhouden van toegangscontrolesystemen. Bedrijven kunnen zich certificeren voor één of meer van de volgende vier onderwerpen:

Onderwerp	Toepassingsgebied	Bedrijf
• Producten	Het leveren van componenten van een toegangscontrolesysteem onder keurmerk	Leverancier Toegangscontrolesystemen
• PvE en projectie	Het leveren van een PvE + projectering van een toegangscontrolesysteem onder keurmerk	Adviesbureau Toegangscontrolesystemen
• Detailontwerp, installatie en opleveren	Het opstellen van het detailontwerp, het installeren en opleveren van een toegangscontrolesysteem onder keurmerk	Technisch Toegangscontrolebedrijf
• Onderhoud	Het leveren van de dienst onderhoud aan een toegangscontrolesysteem onder keurmerk	Onderhoudsbedrijf Toegangscontrolesystemen

De leverancier borgt de onderlinge samenwerking tussen componenten. Het adviesbureau stelt het PvE op en projecteert het toegangscontrolesysteem. Deze projectie is onafhankelijk van een bepaald merk en type toegangscontrolesysteem. Het Technisch Toegangscontrolebedrijf maakt het detailontwerp van het toegangscontrolesysteem in combinatie met de toegepaste componenten. Het is denkbaar dat het Technisch Toegangscontrolebedrijf ook als Adviesbureau optreedt en dan ook het PvE opstelt. Onderhoud wordt uitgevoerd door een onderhoudsbedrijf. De gebruiker is zelf verantwoordelijk voor het op gezette tijden organiseren van het onderhoud.

1.3 Begrippen en afkortingen

- Adviesbureau Toegangscontrolesystemen De partij die het PvE en de projectie van een toegangscontrolesysteem onder keurmerk levert;
- BMI Brandmeldinstallatie;
- Centrale verwerkingseenheid Procesverwerking; veelal elektronisch en met behulp van software. Toegangscontrole is te beheren, te programmeren en de data is op te slaan;
- Cbp College bescherming persoonsgegevens;



- Zone Aaneengesloten gebied binnen de omvang van het Toegangscontrolegebied waarvoor eenzelfde gedefinieerde toegangsclassificatie geldt.

1.4 Classificatie componenten

Voor de classificatie van componenten worden de tabellen uit bijlage X gehanteerd.

1.5 Toegangscontrolegebied (zonering)

Het toegangscontrolegebied beslaat het geheel aaneengesloten gebied waarvoor een bepaalde toegangscontrole geldt. Dit kan dus ook voor een buitengebied gelden; bijvoorbeeld een stadscentrum met selectieve toegangen of een groot bedrijventerrein. Dit buitengebied kan opgedeeld zijn in zones met objecten (zie hiervoor bijlage XI).

Bij plattegronden kan worden gewerkt met de begrippen:

- observatiegebied;
- beveiligd gebied;
- vitaal gebied.

1.6 Koppeling met de regelgeving

Het Bouwbesluit 2003 met de wijzigingen in 2005 heeft raakvlakken met brand- en vluchtveiligheid. In de bijlagen van dit certificatieschema wordt op deze onderwerpen ingegaan. Zie verder voor:

- Inbraakwerendheid : bijlage I;
- Vluchtwegen : bijlage II;
- Brandveiligheid : bijlage III;
- Ontruimingsalarminstallaties : bijlage III.

1.7 Procescertificaat voor de certificaathouder

De CI maakt voor de erkenning van het bedrijf gebruik van een modelverklaring. Dit model is opgenomen in bijlage IV van dit certificatieschema.

1.8 Keurmerk

Het keurmerk dat integraal voor het Keurmerk Elektronisch Toegangsbeheer beschikbaar is ziet er als volgt uit:



1.9 Keurmerk op eindresultaat

Afhankelijk van het onderwerp van certificatie wordt het keurmerk aangebracht op het eindresultaat zoals bijvoorbeeld het PvE of het onderhoudsrapport. De voorschriften zijn per certificatieonderwerp opgenomen in de volgende hoofdstukken.



2 Componenten Toegangscontrole

2.1 Algemeen

In dit hoofdstuk zijn de eisen opgenomen waaraan de componenten van Toegangscontrolesystemen moeten voldoen en welke controles de leverancier moet uitvoeren om aan te tonen dat de productsamenstelling voldoet aan het keurmerk.

2.2 Functionele eisen toegangscontrolesysteem NEN-EN 50133-1

Een Toegangscontrolesysteem bestaat uit diverse (technische) componenten die zo zijn geconfigureerd dat een werkend systeem ontstaat.

Alle componenten die minimaal één van de negen functies vervullen zoals in deze paragraaf aangegeven horen als component bij het toegangscontrolesysteem.

In NEN-EN 50133-1 zijn 9 basisfuncties omschreven die het systeem als geheel moet kunnen vervullen. Te weten:

Basisfunctie	Uitleg
1. Procesverwerking	Centrale verwerkingseenheid Elektronisch Toegangsbeheer, 'CvE ET';
2. Energievoorziening ¹	Voeding met noodstroomvoorziening;
3. Beveiligen ²	Afgeschermd functie naar verwerkingseenheid en interface t.b.v. programmeren;
4. Programmeren	Programeerbare / instelbare toegangscontrole per doorgang;
5. Beheersen	In- en output gegevens beheersbaar per doorgang;
6. Herkennen	Herkenning per doorgang gedefinieerd;
7. Visualiseren / display	(Beeld)schermfunctie voor gebruiker;
8. Informatietransport	Mogelijkheid bieden om gegevens uit de verwerkingseenheid te presenteren aan derden;
9. Communicatie	Mogelijkheid bieden om gegevens uit de verwerkingseenheid te prepareren voor overige dataverwerkingssystemen;

¹Energievoorziening; nader specificatie:

- Netspanningaansluiting (NEN 1010)
- Gelijkspanningsvoorziening
- No-break, 12 uur gangreserve (capaciteitsberekening waarin – indien van toepassing - alle sturingen zijn meegenomen aan de doorgangen)
- Externe signalering bij netspanninguitval en accualarm
- Indien sturingen aan doorgangen niet worden gevoed uit de centrale verwerkingseenheid (bijvoorbeeld bij elektrische deurvergrendelingen) zal ook de externe voeding moeten zijn uitgevoerd met een no-break met 12 uur gangreserve
- Ruststroomprincipe of stroomvoerend naar componenten

²Beveiligen

- Vandalisme en sabotagebestendigheid; vooral bij ruststroomprincipe;
- Sabotagecontacten

2.3 Componenten

Op componentniveau (software, paslezers, centrale verwerkingseenheid, elektrisch gestuurde deurvergrendelingen e.d) zullen de specificaties van de componenten worden onderkent maar niet verder worden uitgewerkt. De componenten zullen waar mogelijk voldoen aan Europese normen en CE zijn gemarkeerd.



2.3.1 Sturingen aan elektrische vergrendelingen

Het toegangscontrolesysteem stuurt veelal gecontroleerd diverse elektrische vergrendelingen aan. Zonder deze vergrendelingen is het praktisch niet mogelijk toegangscontrole te realiseren. Denk hierbij naast de bekende elektrisch gestuurde deurvergrendelingen (slot/sluitplaat/sluitkom) ook aan tourniquets en draaideuren. Het elektronisch toegangscontrolesysteem stuurt deze componenten aan en daarom wordt de 'sturing' wel onderdeel van het installatietechnische gedeelte van dit certificatieschema. Deze componenten zelf zoals de sloten vallen niet onder het keurmerk van de leverancier. Deze componenten worden vaak door derden geproduceerd.

De sturing naar de componenten toe valt wél onder dit certificatieschema. Dit betekent voor de leverancier dat de geïntegreerde productsamenstelling 'stuursignalen' aan moet kunnen bieden aan vergrendelingen.

De exacte specificaties van de stuursignalen moeten door de leverancier worden omschreven in de installatievoorschriften.

Toelichting

Zie verder bijlage I voor meer informatie over de inbraakwerendheid van dergelijke elektrische deurvergrendelingen.

2.4 Classificatie

De leverancier dient aan de hand van de classificatietabellen uit bijlage X de klasse vast te stellen van de geïntegreerde productsamenstelling. De klasse geeft een relatie met het risiconiveau van het object of de locatie.

2.5 Controle op de eisen t.a.v. componenten

De leverancier zal aan de hand van eigen testen, testrapporten van derden, release notes en/of aanvullende technische specificaties moeten vaststellen of de componenten 'werken' op het toegangscontrolesysteem. Dit is met name van belang indien er universele componenten zoals paslezer of tokens worden gebruikt bij integraal werkende systemen.

De leverancier wordt in relatie met het keurmerk verantwoordelijk voor de kwaliteit én de werking van de gehanteerde componenten.

Voor deze productvrijgave dient de leverancier een procedure te hebben die is vastgelegd in het kwaliteitssysteem. De leverancier dient de volledige test of beoordeling van het component te registreren en te archiveren. Dit geldt ook voor het vaststellen van de classificatie.

2.6 Controle op de waarborg en leveringsomvang van de integrale productsamenstelling.

De leverancier dient te verklaren dat de productsamenstelling zoals genoemd in paragraaf 2.2 – mits correct geïnstalleerd – een werkend toegangscontrolesysteem oplevert.

Deze verklaring dient per unieke samenstelling apart te worden afgegeven, schriftelijk beschikbaar te zijn, een overzicht te geven van de gebruikte componenten en te zijn ondertekent door de daarvoor verantwoordelijke medewerker. De leverancier maakt daarbij gebruik van het model dat is opgenomen in bijlage XIII.



Verder dient de leverancier:

- te beschikken over een helpdesk tijdens kantooruren;
- componenten en apparatuur (gelijkwaardig) gedurende 5 jaar te kunnen naleveren;
- trainingen aan te bieden aan de opdrachtgevers en technische toegangscontrolebedrijven over toegangscontrolesystemen die geleverd worden;
- de componenten te classificeren conform bijlage X van dit certificatieschema;
- er instructies en documentatie in de Nederlandse taal bij te leveren;
- installatievoorschriften bij te voegen;
- een onderhoudsvoorschrift bij te voegen.

Toelichting

Indien er bij een project bijvoorbeeld de bestaande paslezers of elektrisch gestuurde deurvergrendelingen worden overgenomen zal de leverancier opnieuw moeten verklaren dat het geheel aan componenten wederom een integraal werkend systeem oplevert. De leverancier wordt in relatie met het keurmerk verantwoordelijk voor de kwaliteit en de werking van de overgenomen componenten.

2.7 Keurmerk op eindresultaat

Op de integraal werkende productsamenstelling brengt de leverancier het keurmerk aan. Dit wordt fysiek aangebracht op de verklaring (document) van de geïntegreerde productsamenstelling (overzicht gebruikte componenten) . Op deze verklaring (specificatieblad) staat de exacte samenstelling van de componenten genoteerd. Deze samenstelling wordt tevens voorzien van een unieke code en ingangsdatum waarop de betreffende productsamenstelling is vrijgegeven voor de leverancier en daarmee voldoet aan de eisen van dit certificatieschema.



3 Eisen aan het PvE en de projectie

3.1 Algemeen

In dit hoofdstuk zijn de eisen opgenomen waaraan het opstellen van het PvE en de projectie van het Toegangscontrolesystemen moeten voldoen. Het opstellen van het PvE en de projectie van het Toegangscontrolesysteem onder keurmerk wordt uitgevoerd door het Adviesbureau Toegangscontrolesystemen.

3.1.1 Kwalificaties

Het opstellen van het PvE en de projectie dient te worden uitgevoerd door personen met het diploma Projecteringsdeskundige Toegangscontrolesystemen.
Voor de overige eindtermen wordt verwezen naar hoofdstuk 6 van dit certificatieschema.

3.1.2 Eisen samenwerking met de opdrachtgever (PvE)

Het Adviesbureau Toegangscontrolesystemen dient inzichtelijk te maken welke eisen de opdrachtgever stelt aan het toegangscontrolesysteem. Het Adviesbureau dient – om de eisen inzichtelijk te maken – gebruik te maken van het standaard Programma van Eisen (PvE) dat is opgenomen in bijlage VIII.

Voor zover er door de opdrachtgever geen eisen stelt dient het bedrijf zelf invulling te geven aan de aspecten die zijn genoemd in het PvE.

Indien er al een vorm van toegangscontrole met een systeem aanwezig is zal moeten worden nagegaan in hoeverre het aanwezige systeem bruikbaar is.

3.1.3 Eisen aan het transmissiesysteem

Afhankelijk van de wensen van de afnemer kan het transmissiesysteem worden uitgevoerd als standaard of met een bepaalde mate van integriteit. Nadere uitleg over beveiligen van de transmissiewegen van digitale systemen zie Bijlage IX.

Standaard: Het transmissiesysteem moet voldoen.

- er een Toegangscontrolesysteem geleverd wordt, waarbij er sprake is van een vaste fysieke kabelverbinding tussen opnemer en verwerkingseenheid, die o.a. voor de doorgifte van de gegevens wordt gebruikt en/of;
- er een Toegangscontrolesysteem geleverd wordt, waarbij er sprake is van een verbinding (niet per definitie vast en fysiek) tussen opnemer en verwerkingseenheid die o.a. voor de doorgifte van gegevens wordt gebruikt.

Integer: Het transmissiesysteem moet voldoende integer zijn.

- er een Toegangscontrolesysteem geleverd wordt, waarbij er sprake is van een vaste fysieke kabelverbinding tussen opnemer en verwerkingseenheid, die exclusief voor de doorgifte van gegevens wordt gebruikt en/of;
- er een Toegangscontrolesysteem geleverd wordt, waarbij er sprake is van een verbinding (niet per definitie vast en fysiek) tussen opnemer en verwerkingseenheid die (niet) exclusief voor de doorgifte van gegevens wordt gebruikt, maar wel voorziet in een beveiliging van het gegevens van opnemer tot en met de verwerkingseenheid.

3.1.4 Eisen aan opgeslagen gegevens

Het bedrijf kan apparatuur leveren ten behoeve van de verwerking en opslag van persoonsgegevens. Als er persoonsgegevens automatisch of gedeeltelijk automatisch worden verwerkt is de wet bescherming persoonsgegevens (Wpb) van kracht.

Het bedrijf dient de afnemer actief te informeren over de eisen die de Wpb stelt.(o.a. aanmelden College bescherming persoonsgegevens; het Cbp).



Als de Wpb van toepassing is zal dit in overleg met de afnemer schriftelijk worden vastgelegd. De afnemer zelf zal ook moeten voldoen aan de eisen die de wetgever stelt ten aanzien van privacy en persoonsgegevens.

De verantwoordelijkheid voor het beheer van de gegevens ligt volledig bij de afnemer.

Indien er een toegangscontrolesysteem geleverd wordt voor de werkwijze van persoonsgegevens zal het bedrijf een systeem aanbieden (software en hardware) die de uitvoering van de wet mogelijk maakt. Het systeem zal daarvoor aan onderstaande randvoorwaarden moeten kunnen voldoen:

- Toegang tot de opgeslagen gegevens (archief) is selectief toegankelijk;
- De gegevens zelf zijn met toegangsrechten vanuit de software selectief toegankelijk;
- De gegevens (personeel) moeten anoniem gemaakt kunnen worden;
- Er mag binnen het toegangscontrolesysteem geen apparatuur of software van derden aanwezig zijn waarmee de gegevens voor, tijdens of na opslag in blijvende zin ongeautoriseerd gemanipuleerd kan worden.

3.1.5 Zelfstandig functionerende toegangscontrolesystemen

Bij zelfstandig functionerende systemen wordt de 'sturing' voor het ontgrendelen van de doorgang door de lezer verzorgd. In de lezer is dan de leeseenheid zelf, aansluiting voor de voedingsspanning en de (eenvoudige) verwerkingsapparatuur.

Als voorbeeld bouwkundige sloten met een codebedieningspaneel. Hiermee is toegangscontrole te organiseren bij een doorgang zonder tussenkomst van centrale apparatuur. Deze vorm van toegangscontrole valt buiten het keurmerk voor de leverancier. Het Adviesbureau Toegangscontrole neemt dit onderwerp echter wel op in het standaard PvE zodat in een later stadium het Technisch Toegangscontrolebedrijf er rekening mee kan houden in het detailontwerp.

3.1.6 Vaststellen PvE

Het Adviesbureau Toegangscontrolesystemen dient het definitieve PvE af te stemmen met de opdrachtgever en de eventuele overige eisende partijen. Na afstemming wordt het PvE aantoonbaar vastgesteld door een daarvoor gekwalificeerde persoon.

Indien het Adviesbureau Toegangscontrolesystemen geen afstemming met de opdrachtgever kan realiseren of reactie van deze uitblijft dient het Adviesbureau Toegangscontrolesystemen het PvE vast te stellen en te bevestigen naar de opdrachtgever dat dit PvE gerealiseerd gaat worden.

Wijzigingen die naderhand op het plan worden doorgevoerd dienen wederom conform deze paragraaf te worden afgestemd en aansluitend te worden vastgesteld voordat tot uitvoering kan worden overgegaan.

In het PvE worden geen merk(namen) genoemd.

3.2 Projectie

Op basis van het PvE wordt een projectie gemaakt. Het resultaat van de projectie omvat een overzichtstekening met daarop aangegeven :

- De omvang van het toegangscontrolesysteem. (aantal gebouwen, bouwlagen, doorgangen, zones);
- De afbakening van het gebied waarvoor het toegangscontrolesysteem bedoeld is;
- Alle doorgangen met de classificatie en type identificatiemiddel.

Toelichting

De overzichtstekening hoeft niet op het niveau van het aansluitschema te worden uitgewerkt. De tekening moet kunnen worden uitgewerkt door de Technisch Toegangscontrolebedrijven die de specifieke producttrainingen hebben gehad van de leverancier.



Tevens zal het Adviesbureau Toegangscontrolesystemen met documenten (schriftelijk) moeten kunnen onderbouwen hoe tot de projectie is gekomen. De volgende aspecten zijn in deze onderbouwing beschreven:

- Toegangsgroepen – aantallen;
- Tijdroosters – aantallen;
- Organisatorische maatregelen;
- Bouwkundige maatregelen;
- Elektronische maatregelen;
- Consequenties inbraakwerendheid, brandveiligheid en vluchtveiligheid.

De toepassing én locatie van elektrische vergrendelingen zal worden meegenomen in de projectie. In de projectie worden geen merk(namen) genoemd

3.2.1 Vaststellen projectering

Het Adviesbureau Toegangscontrolesystemen dient de definitieve projectie aantoonbaar vast te stellen door een daarvoor gekwalificeerde persoon.

Wijzigingen die naderhand op de projectie worden doorgevoerd dienen wederom conform deze paragraaf te worden doorgevoerd en aansluitend te worden vastgesteld voordat tot uitvoering kan worden overgegaan.

3.3 Keurmerk op eindresultaat

De Adviesbureau Toegangscontrolesystemen brengt op het PvE en de projectie van het toegangscontrolesysteem het keurmerk zichtbaar aan. Dit wordt fysiek aangebracht op de documenten. Het PvE en de projectie worden tevens voorzien van een unieke code en datum waarop het betreffende PvE en projectie is gevalideerd en voldoet aan de eisen van dit certificatieschema.



4 Eisen aan het detailontwerp, installeren en opleveren

4.1 Algemeen

In dit hoofdstuk zijn de eisen opgenomen waaraan het installeren en opleveren van Toegangscontrolesystemen moeten voldoen. Het detailontwerp, de installatie en het opleveren van Toegangscontrolesysteem onder keurmerk wordt uitgevoerd door het Technisch Toegangscontrolebedrijf.

4.2 Kwalificaties

Het vaststellen van het detailontwerp dient te worden uitgevoerd door een TBV'er. De installatiewerkzaamheden worden verricht door een MBV'er. Oplevering aan de opdrachtgever wordt uitgevoerd door een TBV'er. De eisen waaraan deze personen moeten voldoen zijn vastgesteld in hoofdstuk 6 van dit schema.

4.3 Opstellen detailontwerp

Het Technisch Toegangscontrolebedrijf maakt op basis van de uitgangspunten zoals zijn vastgelegd in het PvE en de projectie een detailontwerp van het toegangscontrolesysteem. In het detailontwerp wordt vastgelegd welke producten er gebruikt gaan worden voor het toegangscontrolesysteem. Hierbij maakt het bedrijf gebruik van de overzichtstekening die is opgesteld door het Adviesbureau Toegangscontrolesystemen.

Het detailontwerp zal op aansluitniveau van de componenten zijn uitgewerkt. Ook de exacte routing van de bekabeling zal zijn aangegeven in het detailontwerp. Verder dient het Technisch Toegangscontrolebedrijf aan te geven waar en welke elektrische deurvergrendelingen worden toegepast. Hiertoe maakt het bedrijf een keuze uit merk en type en stelt vast of de vergrendeling geen afbreuk doet aan het beveiligingsniveau dat is vereist bij de doorgang. (zie ook bijlage I voor informatie).

Het detailontwerp wordt vastgesteld door een TBV'er.

4.4 Controle voor uitvoering

4.4.1 Controle eisen integraal werkende productsamenstelling

De MBV'er dient op locatie te verifiëren en te registreren of aan de functionele eisen wordt voldaan. Dat kan door middel van het keurmerk dat door de leverancier op de geïntegreerde productsamenstelling is afgegeven.

4.4.2 Controle vastgesteld PvE en projectering

De MBV'er controleert en stelt vast dat het definitieve PVE en de definitieve projectie van het toegangscontrolesysteem, voorzien van het keurmerk, aanwezig is op locatie. De projectie dient in de vorm van een overzichtstekening te zijn uitgevoerd. (plattegrondtekening).

4.4.3 Controle elektrische vergrendelingen

De MBV'er controleert voor aanvang van de werkzaamheden of de elektrische vergrendelingen voldoen aan de eisen die zijn opgenomen in het detailontwerp.

4.5 Uitvoering

Het Technisch Toegangscontrolebedrijf draagt ervoor zorg dat de gebruikte componenten en apparatuur wordt geïnstalleerd en gecontroleerd conform de bijgeleverde voorschriften van de leverancier.



De uitvoering staat onder directe leiding van een MBV'er die op het werk aanwezig is. Deze MBV'er houdt tijdens de uitvoering een overzicht bij van medewerkers, ingehuurd personeel en personeel van onderaannemers die op of aan de installatie werkzaamheden hebben verricht.

Bij de uitvoering dienen de onderstaande uitgangspunten door het Technisch Toegangscontrolebedrijf te worden gerealiseerd om een toegangscontrolesysteem op een basisniveau te brengen:

- elektrische meerpuntsvergrendeling op de buitenschil;
- deuropenstandsignalering op minimaal de doorgangen in de buitenschil;
- vaststellen (on)mogelijkheden van aanpassingen aan branddeuren bij het plaatsen van hang- en sluitwerk voor elektrische vergrendelingen;
- groene handmelder bij nooduitgangen wordt altijd dubbelpolig uitgevoerd (1 voor ontgrendelen en 1 voor signalering);
- bekabeling is niet direct zichtbaar en niet eenvoudig bereikbaar buiten het beveiligde gebied;
- altijd een (beveiligde) voorziening aanbrengen zodat men het object binnen kan komen buiten het toegangscontrolesysteem om.

Het Technisch Toegangscontrolebedrijf kan werkzaamheden, zoals het installatiewerk, uitbesteden. Hiertoe zal zij zich als eindverantwoordelijke houden aan de eisen die zijn opgenomen in hoofdstuk 6 van dit certificatieschema.

4.6 Controle op uitvoering

Een MBV'er controleert en stelt vast dat de installatie van componenten volgens de installatievoorschriften van de betreffende leverancier wordt uitgevoerd.

Hiertoe voert de MBV'er de onderstaande controles uit. Registratie van de controle vindt plaats op een model opleverchecklist. Zie hiervoor bijlage VII.

4.6.1 Controle werking doorgangen

De MBV'er dient alle doorgangen te controleren die onderdeel zijn van het toegangscontrolesysteem. Hierbij controleert de MBV'er de correcte werking van de doorgangverlening. Hiervoor geldt het volgende:

- Als doorgangen correct ontgrendelen en vergrendelen is dat de indicatie voor correct werken. Elektrisch gestuurde deurvergrendelingen (slot/sluitplaat/sluitkom) maken onderdeel uit van deze controle;
- Indien de fysieke vergrendelingen nog niet zijn geïnstalleerd (bijvoorbeeld bij draaideuren) dan controleert de MBV'er of het stuursignaal correct wordt aangeboden vanuit de centrale verwerkingseenheid.

De resultaten van deze controle dienen per doorgang te worden geregistreerd.

De uitvoering van de controle dient met het type identificatiemiddel uitgevoerd te worden dat is vastgesteld in de projectie en het merk dat is vastgesteld in het detailontwerp.

4.6.2 Controle op de eisen van het transmissiesysteem

Een standaard transmissiesysteem wordt niet nader gecontroleerd. Als het toegangscontrolesysteem voldoet aan de eisen in het PvE is het akkoord. Als een transmissiesysteem integer moet zijn uitgevoerd zijn er twee opties:

Vaste kabelverbinding:

De MBV'er controleert een toegangscontrolesysteem waarbij er sprake is van een vaste fysieke kabelverbinding tussen opnemer en verwerkingseenheid, die exclusief voor de doorgifte van gegevens wordt gebruikt, middels de tekening van het toegangscontrolesysteem en de realisatie daarvan in uitvoering. De tekening moet het toegangscontrolesysteem in zijn totaliteit weergeven en hieruit moet blijken dat er op geen enkele manier interactie is met andere apparatuur en/of transmissieweg. Tijdens de uitvoering moet vastgesteld worden dat het ontwerp ook daadwerkelijk in de praktijk wordt gerealiseerd.



Draadloos:

Bij een toegangscontrolesysteem waarbij er sprake is van een verbinding (niet per definitie vast en fysiek) tussen opnemer en verwerkingseenheid die (niet) exclusief voor de doorgifte van gegevens wordt gebruikt, moet gecontroleerd worden of de beveiliging van de gegevens van de opnemer tot en met de verwerkingseenheid afdoende is gerealiseerd. Dit is het geval wanneer kan worden vastgesteld dat er conform bijlage IX is gewerkt. De MBV'er controleert dit.

4.6.3 Controle op de eisen aan opgeslagen gegevens

Deze controle is alleen van toepassing indien het Toegangscontrolesysteem moet voldoen aan de randvoorwaarden die gelden voor de verwerking van persoonsgegevens zoals omschreven in de Wbp. De MBV'er controleert en registreert op locatie of wordt voldaan aan onderstaande randvoorwaarden:

- toegang tot de opgeslagen gegevens (archief) is selectief toegankelijk;
- de gegevens zelf zijn selectief toegankelijk;
- de gegevens (personeel) moeten anoniem gemaakt kunnen worden;
- er mag binnen het toegangscontrolesysteem geen apparatuur of software van derden aanwezig zijn waarmee de gegevens voor, tijdens of na opslag in blijvende zin gemanipuleerd kunnen worden.

4.6.4 Controle wijzigingen overzichtstekening

De MBV'er controleert of er wijzigingen zijn in de uitvoering waardoor de overzichtstekening moet worden aangepast. Bij de oplevering aan de klant dienen alle wijzigingen op de tekening te zijn doorgevoerd.

Het Technisch Toegangscontrolebedrijf geeft aantoonbaar de wijzigingen door aan het Adviesbureau Toegangscontrolesystemen dat het PVE en de projectie heeft opgesteld.

4.6.5 Controle op overige eisen

Indien de afnemer nadere eisen heeft gesteld aan het toegangscontrolesysteem dienen deze te zijn opgenomen in het PvE. De controle op de eisen zal daarop afgestemd moeten worden en kan maatwerk zijn. De MBV'er controleert dit.

4.7 Inbedrijfstelling en opleveren

Na vaststelling dat alle controles een positief resultaat hebben levert de TBV'er het toegangscontrolesysteem op en draagt het systeem over aan de opdrachtgever; bij voorkeur aan de opgeleide persoon (OP-er).

Bij de oplevering dient de definitieve overzichtstekening gereed te zijn.

Bij de oplevering verstrekt de TBV'er aan de opdrachtgever:

- Het definitieve PvE en overzichtstekening;
- Een (kopie van) de ingevulde en afgetekende opleverchecklist die bij de controle volgens bijlage VII van dit certificatieschema;
- Eventuele randvoorwaarden en gebruiksaanwijzingen die behoren bij het Toegangscontrolesysteem of onderdelen ervan;
- Een onderhoudsschema dat de opdrachtgever dient aan te houden.

4.8 Oplevercertificaat Toegangscontrolesystemen

Het oplevercertificaat is het document dat het Technisch Toegangscontrolebedrijf afgeeft aan haar klanten bij oplevering van een toegangscontrolesysteem bij een nieuw te installeren toegangscontrolesysteem.

Binnen twee werkweken na oplevering van de werkzaamheden maakt het Technisch Toegangscontrolebedrijf het oplevercertificaat toegangscontrolesystemen op en geeft hiervan een exemplaar af aan de opdrachtgever en houdt zelf ook een exemplaar. Hierbij maakt het bedrijf gebruik van een door het College van Deskundigen vastgesteld model dat is opgenomen in Bijlage V. Een oplevercertificaat is altijd gekoppeld aan een getekend PvE van de installatie. De TBV'er tekent dit certificaat zelf.



Dit oplevercertificaat weerspiegelt een momentopname en krijg wel een datum van afgifte maar geen verloopdatum. Een drietal zaken die voor de gebruiksfase van belang zijn zullen aanvullend op dit certificaat worden vermeld:

1. De gebruikers van het elektronische toegangscontrolesysteem moeten voor het beheer een daartoe opgeleide persoon inzetten; een opgeleid persoon zorgt ervoor dat de werking van het elektronische toegangscontrolesysteem volledig tot zijn recht komt en weet wanneer de hulp van specialisten noodzakelijk is.
2. Voor de goede en betrouwbare werking van het toegangscontrolesysteem is het van belang dat er periodiek onderhoud wordt uitgevoerd door een bedrijf dat daartoe gecertificeerd is. Het wordt aanbevolen om onderhoud jaarlijks te laten uitvoeren.
3. Uitbreiding van of bouwkundige wijzigingen in het gebouw kunnen altijd effect hebben op een goede en betrouwbare werking van het elektronische toegangscontrolesysteem. Dit geldt ook als het gebruik van het gebouw (of delen ervan) wijzigt. De gebruiker wordt geadviseerd om in al deze gevallen contact op te nemen met een bedrijf dat gecertificeerd is voor het opstellen van PvE's en projecteren. In onderling overleg kan bepaald worden of het noodzakelijk is dat er daadwerkelijk een nieuw PvE en/of ontwerp wordt gemaakt.

4.9 Keurmerk op eindresultaat

Detailontwerp

Het Technisch Toegangscontrolebedrijf brengt het keurmerk zichtbaar op het detailontwerp van het toegangscontrolesysteem aan. Dit wordt fysiek aangebracht op de documenten. Het detailontwerp wordt tevens voorzien van een unieke code en datum waarop het betreffende detailontwerp is gevalideerd en voldoet aan de eisen van dit certificatieschema.

Installatie

Op het oplevercertificaat is het keurmerk aangebracht. Zie daarvoor bijlage V van dit certificatieschema.



5 Eisen aan het onderhouden

5.1 Algemeen

In dit hoofdstuk zijn de eisen opgenomen waaraan de dienst onderhoud van Toegangscontrolesystemen moeten voldoen. Het onderhoud aan een Toegangscontrolesysteem onder keurmerk wordt uitgevoerd door het Onderhoudsbedrijf Toegangscontrolesystemen.

5.2 Kwalificaties

Het onderhoud aan toegangscontrolesystemen dient te worden uitgevoerd door een MBV'er (MBV = opleiding monteur beveiligingsinstallaties; relatie met de BORG Inbraak regeling). Voor de overige eindtermen wordt verwezen naar hoofdstuk 6 van dit certificatieschema.

5.3 Onderhoud

Bij de start van het onderhoud controleert het onderhoudsbedrijf het 'Oplevercertificaat Toegangscontrolesystemen' van het betreffende Toegangscontrolesysteem. Het onderhoud wordt uitgevoerd volgens het onderhoudsschema dat behoort bij het betreffende Toegangscontrolesysteem. Onderhoud vindt verder plaats door vast te stellen dat het Toegangscontrolesysteem niet is/wordt gewijzigd of uitgebreid aan de hand van het PvE en de overzichtstekening van het systeem dat op locatie aanwezig moet zijn. Het onderhoudsbedrijf maakt van het uitgevoerde onderhoud een rapport op. Hiervoor wordt gebruikt gemaakt van het model dat is opgenomen in Bijlage XII van dit certificatieschema.

Het onderhoudsbedrijf controleert 100% van de doorgangen. Deze controle dient aan de hand van de overzichtstekening van het toegangscontrolesysteem. De uitvoering dient met het type identificatiemiddel uitgevoerd te worden die is vastgesteld in de projectie en het merk dat is vastgesteld in het detailontwerp.

Het onderhoudsbedrijf controleert de correcte werking van de doorgangverlening. Hiervoor geldt het volgende:

- Als doorgangen correct ontgrendelen en vergrendelen is dat de indicatie voor correct werken. Elektrisch gestuurde deurvergrendelingen (slot/sluitplaat/sluitkom) maken onderdeel uit van deze controle;
- Bij fysieke (bouwkundige) vergrendelingen (bijvoorbeeld bij draaideuren) wordt minimaal het bepaald of het stuursignaal correct wordt aangeboden vanuit de centrale verwerkingseenheid.

De resultaten van deze controle dienen per doorgang te worden geregistreerd op de onderhoudsrapportage. Alle beoordelingen moeten positief zijn.

In geval er een afwijking wordt vastgesteld moet het Toegangscontrolesysteem binnen specificatie worden gebracht door alleen het vervangen van componenten. Indien dit betekent dat het PvE en de projectie moeten worden herzien dat geeft het onderhoudsbedrijf deze wijzigingen aantoonbaar door aan het Adviesbureau Toegangscontrolesystemen dat het PvE en de projectie heeft opgesteld.

Uitbreidingen, bouwkundige wijzigingen of veranderd gebruik van een gebouw leiden altijd tot het aanpassen van een herbeoordeling van een PvE en projectie. Aan Toegangscontrolesysteem zonder een oplevercertificaat Toegangscontrolesystemen mag geen onderhoud onder keurmerk worden uitgevoerd.

5.4 Onderhoudsrapport na onderhoud

Binnen twee weken na de onderhoudswerkzaamheden maakt het onderhoudsbedrijf een onderhoudsrapport op. Het onderhoudsbedrijf geeft één exemplaar af aan de opdrachtgever en houdt zelf ook een exemplaar.



5.5 **Keurmerk op eindresultaat**

Op het onderhoudsrapport is het kenmerk aangebracht. Zie voor het model van het onderhoudsrapport bijlage XII van dit certificatieschema.



6 Eisen aan het kwaliteitssysteem

6.1 Algemeen

In dit hoofdstuk staan de eisen waaraan het kwaliteitssysteem van de certificaathouders aan moeten voldoen. Er worden op basis van het onderwerp van certificatie vier certificaathouders onderscheiden: de Leverancier, Adviesbureau, Technisch Toegangscontrolebedrijf en de Onderhoudsbedrijf. Per certificaathouder is in de tabel hieronder aangegeven welke paragrafen uit hoofdstuk 6 van toepassing zijn:

Paragraaf	Leverancier	Adviesbureau	Technisch Toegangscontrolebedrijf	Onderhoudsbedrijf
6.2	X	X	X	X
6.3	X	X	X	X
6.4	X	X	X	X
6.5	X	X	X	X
6.6	X	X	X	X
6.6.1			X	
6.7.1	X	X	X	X
6.7.2	X	X		
6.7.3			X	X
6.7.4			X	
6.8	X	X	X	X
6.7	X	X	X	X
6.8	X	X	X	X
6.9	X	X	X	X
6.10	X	X	X	X
6.11	X	X	X	X
6.12	X	X	X	X
6.13			X	

6.2 Borging eisen uit dit beoordelingsschema

Het bedrijf maakt een kwaliteitssysteem gericht op het onderwerp van certificatie waarvoor het is gecertificeerd. Te weten:

Certificaathouder	Onderwerp van certificatie
Leverancier Toegangscontrolesystemen	Producten
Adviesbureau Toegangscontrolesystemen	PvE en projectie
Technisch Toegangscontrolebedrijf	Detailontwerp, installatie en opleveren
Onderhoudsbedrijf Toegangscontrolesystemen	Onderhoud

Het kwaliteitssysteem omvat naast de in dit hoofdstuk vermelde eisen minimaal de volgende onderwerpen:

- Organogram;
- Kwaliteitsbeleid;
- Offertes, opdracht- en contractvorming;



- Opleiding, bijscholing en evaluatie van het personeel in de praktijk;
- Aanwezigheid van documentatie bij aanvang installatiewerk en/of onderhoud;
- Gebruik van het kenmerk van het keurmerk (pictogram);
- Controle op het uitgevoerde werk (van de dienst) met goed- en afkeurcriteria voor het uitgevoerde werk (van de dienst);
- Rapportage van uitgevoerde installatiewerk en/of onderhoud;
- Afgeschermd beheren vertrouwelijke klantgegevens tijdens de projecten;
- Inhuren van personeel;
- Uitbesteden van werk;
- Nauwkeurigheid en kalibratie van meetinstrumenten;
- Behandeling van klachten;
- Correctie(s) en corrigerende maatregelen;
- Documentbeheer (registraties, archief, personeelsdossiers etc);

Het bedrijf maakt een overzichtsschema, waaruit blijkt dat ieder onderdeel van dit certificatieschema correspondeert met een onderdeel van het kwaliteitssysteem.

Dit schema is minimaal tot op paragraafniveau van dit certificatieschema uitgewerkt.

De documentatie van het bedrijf is voorzien van een index met ingangsdatum, versienummer en validatie door de eindverantwoordelijke persoon.

6.3 Beheerder van het kwaliteitssysteem

Binnen de organisatiestructuur van het bedrijf moet een functionaris zijn aangewezen die belast is met het beheer van het kwaliteitssysteem.

6.4 Taken, verantwoordelijkheden en bevoegdheden

Alle medewerkers van het bedrijf die bij de eisen van dit certificatieschema betrokken zijn, dienen, voor zover relevant voor hun werkzaamheden in relatie tot de vereiste kwaliteit, op de hoogte te zijn van de inhoud van het kwaliteitssysteem, de eigen taken, verantwoordelijkheden en bevoegdheden.

6.5 Procedures en werkinstructies

Het bedrijf moet kunnen overleggen:

- procedures voor:
 - o Het vrijgeven van producten/diensten zoals genoemd in dit certificatieschema;
 - o de behandeling van producten/diensten met afwijkingen;
 - o corrigerende maatregelen bij geconstateerde tekortkomingen;
 - o de behandeling van klachten over geleverde producten en/of diensten;
- de gehanteerde werkinstructies en controleformulieren (zoals eventuele checklisten).

6.6 Opdrachtvorming

In aanbiedingen naar potentiële opdrachtgevers maakt het bedrijf duidelijk dat het onderwerp van certificatie (zie paragraaf 1.2 toepassingsgebied) geleverd gaat worden volgens dit certificatieschema.

6.6.1 Extra eis opdrachtvorming voor het Technisch Toegangscontrolebedrijf

Het Technisch Toegangscontrolebedrijf dient de volgende tekst duidelijk aan de aanbieder toe te voegen:

“het Toegangscontrolesysteem is ontworpen en wordt geïnstalleerd volgens de eisen zoals omschreven in het certificatieschema ‘Keurmerk Elektronisch Toegangsbeheer’.

6.7 Vakbekwaamheid en Kwalificaties

In deze paragraaf zijn de eindtermen vastgesteld waaraan personeel en/of instanties moeten voldoen. Het bedrijf moet aantoonbaar maken dat een medewerker aan de betreffende eis voldoet door een diploma te overleggen dat is afgegeven door een instantie of bedrijf dat examens afneemt.

6.7.1 Instantie die examens afneemt

Deze instantie beschikt aantoonbaar over een, door de directie of bestuur, vastgesteld reglement waarin de volgende zaken zijn geregeld:



- de verantwoordelijkheid van de bij het examen betrokken partijen;
- een ieder die dat wil heeft toegang tot het examen heeft zonder dat hier andere verplichtingen aan worden gekoppeld;
- procedures voor inschrijving;
- controle op de identiteit van de kandidaten
- tijdafspraken over het examen;
- toezicht tijdens het examen;
- sanctiemaatregelen (gericht op fraude en (te)laatkomers);
- de procedure voor beroep inzake de uitslag van het examen;
- de procedure voor een herexamen.

Dit reglement dient van toepassing te zijn op het examen en wordt door een examenorganisatie ter beschikking gesteld aan de CI. Alle examenorganisaties dienen verder een modeldiploma aan de CI ter beschikking te stellen.

6.7.2 Projecteringsdeskundige Toegangscontrolesystemen

- Diploma Projecteringsdeskundige Elektronische Toegangsbeheer; Eindtermen: SSQ
- Trainingen door de leverancier van toegangscontrolesystemen die door de projecteringsdeskundige worden geprojecteerd
- Kennis hebben van beveiligingstechnieken van deuren en doorgangen
- Kennis hebben van vluchtveiligheid in gebouwen
- Kennis hebben van brandmeldinstallaties en ontruimingsalarminstallaties in relatie tot toegangscontrolesystemen
- Verklaring van betrouwbaarheid

6.7.3 MBV'er

- Diploma opleiding monteur beveiligingsinstallaties MBV;
- Trainingen door de leverancier van toegangscontrolesystemen die door de MBV'er worden geïnstalleerd.

Bij gebruikmaking van IP-technieken dienen de betrokken medewerkers te beschikken over een opleiding met als onderwerp "IP-technieken en beveiliging". Van de relevante functies zullen de opleidingseisen worden vastgesteld en worden vastgelegd op welke wijze het kennis en opleidingsniveau wordt geborgd.

6.7.4 TBV'er

- Diploma opleiding monteur beveiligingsinstallaties TBV
- Trainingen door de leverancier van toegangscontrolesystemen die de TBV'er ten behoeve het detailontwerp en de oplevering nodig heeft om het werk goed te kunnen uitvoeren.

6.8 Integriteit personeel – ter informatie

Uitgangspunt bij het werk met data van toegangscontrolesystemen is het feit dat deze vertrouwelijk zijn. De gegevens van personen is door het toegangscontrolesysteem inzichtelijk.

Er worden in dit certificatieschema eisen gesteld aan de 'integriteit' van het eigen personeel dat direct betrokken is bij of belast is met uitvoering van het werk omschreven in dit certificatieschema.

Voor eigen personeel wordt daarom een verklaring van betrouwbaarheid aangevraagd. (Aanvragen bij politie in de gemeente waar het personeelslid woont).

Indien zich zeer informatiegevoelige projecten voordoen kan het zinvol zijn vanuit de interne organisatie procedures op te stellen hoe met deze projectdossiers wordt gegaan.

6.9 Uitbesteden van werk en inhuur van personeel

Het bedrijf mag werk uitbesteden en personeel inhuren om de werkzaamheden te verrichten. Het bedrijf maakt in beide situaties aantoonbaar dat medewerkers aan de eisen voldoen. Personeel dat wordt ingehuurd moet verder volledig aan dezelfde eisen voldoen als het eigen personeel.



Wanneer er werk wordt uitbesteed zorgt het bedrijf ervoor dat een eigen medewerker, die aan de kwalificaties voldoet, continue toezicht houdt. Dit laatste geldt niet bij uitbesteding aan ander bedrijf dat beschikt over een certificaat voor hetzelfde onderwerp van certificatie op basis van dit certificatieschema.

6.10 Documentenbeheer

Het bedrijf dient te beschikken over de volgende documenten:

- dit certificatieschema;
 - het eigen kwaliteitssysteem (op papier of elektronisch);
 - alle normatieve documenten zoals vermeld in paragraaf 8.1;
 - resultaten van alle uitgevoerde controles;
 - informatie over gebruikte producten,
- en ervoor te zorgen dat deze documenten beheerd worden.

6.11 Klachten en corrigerende maatregelen – niet zijnde storingen

Het bedrijf zorgt voor een procedure voor klachten en corrigerende maatregelen. Klachten worden door het bedrijf binnen 2 weken schriftelijk bevestigd. Uiterlijk na twee maanden zorgt het bedrijf ervoor dat de klacht is afgehandeld. De klager ontvangt schriftelijk bericht over de klachtafhandeling. Hierin vermeldt het bedrijf of de klacht terecht was en zo ja welke corrigerende maatregel het bedrijf gaat nemen of genomen heeft.

Verder besluit het bedrijf of verdergaande interne maatregelen nodig zijn om herhaling van de klacht te voorkomen.

6.12 Archivering

Het bedrijf archiveert voor een periode van 5 jaar alle gegevens en registraties die betrekking hebben op de eisen zoals gesteld in dit certificatieschema.

Vertrouwelijke (klant)gegevens moeten vertrouwelijk worden behandeld. De gegevens moeten afgeschermd worden opgeslagen en gearchiveerd.

Toelichting

Wettelijk gezien kunnen er langere bewaartermijnen gelden.

6.13 Melden projecten aan de CI – Alleen voor het installatiebedrijf

Het bedrijf meldt minimaal 5 werkdagen voor de aanvang van de werkzaamheden ieder project aan bij de certificerende instelling. Hiervoor maakt het installatiebedrijf gebruik van het model zoals is opgenomen in bijlage VI.



7 Afspraken over de uitvoering van certificatie

7.1 Algemeen

In dit hoofdstuk zijn de in het College van Deskundigen gemaakte afspraken over de uitvoering van certificatie door de CI vastgelegd. Er worden op basis van het onderwerp van certificatie vier certificaathouders onderscheiden: de Leverancier, Adviesbureau, Technisch Toegangscontrolebedrijf en het onderhoudsbedrijf.

Het certificatieonderzoek is te splitsen in twee onderdelen.

- Het initiële certificatieonderzoek om te komen tot certificatie.
- Na certificatie volgen er periodieke opvolgingsaudits om vast te stellen of het bedrijf blijvend aan de eisen voldoet.

Van iedere uitgevoerde audit wordt door de CI rapport opgemaakt.

7.2 Initieel certificatieonderzoek - samenvatting

Hfdstuk	Leverancier	Adviesbureau	Technisch Toegangscontrolebedrijf	Onderhoudsbedrijf
Hfdstk 2	X			
Hfdstk 3		X		
Hfdstk 4			X	
Hfdstk 5				X
Hfdstk 6	Zie tabel H6	Zie tabel H6	Zie tabel H6	Zie tabel H6

Het onderzoek wordt altijd gestart met de audit van het gedocumenteerde kwaliteitsstelsel.

Aansluitend worden de relevante eisen geaudit op basis van praktijkperformance. In de bovenstaande tabel staan de eisen die de CI per certificaathouder moet toetsen. De CI beoordeelt hierbij per:

- Leverancier: minimaal 3 door de leverancier gevalideerde geïntegreerde productsamenstellingen;
- Adviesbureau: minimaal 3 door het adviesbureau vastgestelde PvE's en projecties;
- Technisch Toegangscontrolebedrijf: minimaal 2 vastgestelde detailontwerpen en 2 compleet geïnstalleerde toegangscontrolesystemen op locatie;
- Onderhoudsbedrijf: minimaal 2 onderhoudsprojecten op locatie.

Alle eisen uit dit certificatieschema voor het onderwerp van certificatie van de betreffende certificaathouder moeten door de CI positief zijn beoordeeld voordat tot certificatie kan worden overgegaan. Indien dit niet het geval is moet het bedrijf corrigerende maatregelen treffen. Aansluitend moet de CI het onderzoek uitbreiden om vast te stellen of alle eisen dan wel positief worden beoordeeld.

7.3 Opvolgingsaudit – samenvatting

Het onderzoek wordt uitgevoerd aan de hand van de relevante eisen uit de tabel van paragraaf 7.2. De CI beoordeelt hierbij per:

- Leverancier: jaarlijks minimaal 3 door de leverancier gevalideerde geïntegreerde productsamenstellingen;
- Adviesbureau: jaarlijks minimaal 3 door het adviesbureau vastgestelde PvE's en projecties;
- Technisch Toegangscontrolebedrijf: jaarlijks 1: 10 (met een minimum van 1) vastgestelde detailontwerpen en 1: 10 (met een minimum van 1) compleet geïnstalleerde toegangscontrolesystemen op locatie;
- Onderhoudsbedrijf: jaarlijks 1: 10 (met een minimum van 1) onderhoudsprojecten op locatie.



Alle eisen uit dit certificatieschema voor het onderwerp van certificatie van de betreffende certificaathouder moeten door de CI positief zijn beoordeeld zijn. Indien dit niet het geval is moet het bedrijf corrigerende maatregelen treffen.

7.4 Certificatiepersoneel

De auditoren die door de CI worden ingezet voor het certificatieonderzoek voldoen aan de volgende eisen:

- Werk - en denkniveau dat gelijk is aan hoger beroepsonderwijs, aantoonbaar door middel van minimaal een HBO diploma of met MBO diploma met drie jaar werkervaring als auditor;
- Kennis van het certificatieschema 'Keurmerk Elektronisch Toegangbeheer' en relevante wetgeving; vastgesteld door de direct leidinggevende van de auditor en geregistreerd in het interne kwaliteitssysteem van de CI;
- kennis van de techniek van toegangscontrolesystemen; aantoonbaar door middel van werkervaring in elektronische toegang- en/of inbraaksystemen en/of auditor voor toegangscontrole en/of werknemer bij een van de vier genoemde type bedrijven in het toepassingsgebied;
- Minimaal twee jaar aantoonbare auditervaring met technische certificatieschema's als gekwalificeerd auditor.

Het bij certificatie betrokken personeel is te onderscheiden naar:

- Certificatiedeskundigen: belast met de coördinatie en beheer van een certificatieschema;
- Auditor: belast met de uitvoering van het toelatingsonderzoek en de controle na certificaatverlening bij het bedrijf; de certificatiedeskundige kan ook als auditor optreden;
- Beslissers (direct leidinggevende auditor/certificatiedeskundige): belast met het nemen van beslissingen naar aanleiding van uitgevoerde toelatingsonderzoeken, voortzetting van certificatie naar aanleiding van uitgevoerde controles en beslissingen over de noodzaak tot het treffen van corrigerende maatregelen.

Opleiding en ervaring van het betrokken certificatiepersoneel moet aantoonbaar zijn vastgelegd.

7.5 Corrigerende maatregelen

Indien er afwijkingen zijn vastgesteld ten aanzien van de eisen, dan corrigeert het bedrijf deze en legt deze - binnen 2 maanden van vaststelling - ter beoordeling voor aan de CI. De CI stelt eveneens binnen 2 maanden vast dat of de correcties afdoende zijn. Bij uitblijven van corrigerende maatregelen, niet effectieve corrigerende maatregelen of het herhaaldelijk optreden van dezelfde afwijkingen neemt de CI afdoende sancties tegen de certificaathouder.

7.6 Rapportage aan College van Deskundigen

De CI rapporteert jaarlijks aan het College van Deskundigen over de activiteiten zoals omschreven in dit hoofdstuk.

In deze rapportage dienen minimaal de volgende aspecten tot uiting te komen:

- het aantal gecertificeerde bedrijven per 1 januari van het betreffende jaar;
 - het aantal certificaten dat in het kalenderjaar er bij is gekomen en dat is opgezegd;
 - een verantwoording van de af te leggen aantallen opvolgingsaudits per certificaat;
 - het aantal en soort sancties jegens de certificaathouders per categorie van sancties met daarbij de onderliggende redenen;
 - verbetervoorstellen van de eisen naar aanleiding van genomen sancties jegens certificaathouders (minimaal 2 voorstellen moeten worden ingediend);
 - knelpunten die zich in de praktijk voordoen en het certificatieschema aanpassing zou behoeven.
- De CI behandelt certificaathouders in deze rapportage anoniem en niet individueel (in verband met de geheimhoudingsplicht van de CI).

Indien het Centraal College van Deskundigen besluit om voor deze rapportage een model op te stellen, dan zullen de CI's dit hanteren.



8 Lijst van vermelde documenten

8.1 Normatieve documenten:

NEN-EN 50133-1	Alarmsystemen - Toegangsbewakingssystemen voor beveiligingstoepassingen - Deel 1: Systeemeisen - www.nen.nl	1996
Certificatieschema KET	Certificatieschema – Keurmerk Elektronisch Toegangsbeheer – www.ssq.nu	2008
Brandbeveiligingsinstallaties - NVBR	Brandpreventieve installatietechnische voorzieningen - www.nvbr.nl	2005
Wet bescherming persoonsgegevens	regels voor een zorgvuldige omgang met persoonsgegevens - http://wetten.overheid.nl	2001

8.2 Informatieve documenten

NEN-EN 12209-3	Hang- en sluitwerk - Sloten en grendels - Deel 3: Elektromagnetisch bediende sloten en sluitplaten - Eisen en beproevingsmethoden	1998
NEN-EN 14846	Hang- en sluitwerk - Sloten en grendels - Elektromagnetisch bediende sloten en sluitplaten - Eisen en beproevingsmethoden	2003
NEN-EN 50133-2-1:2000	Alarmsystemen - Toegangsbewakingssystemen voor beveiligingstoepassingen - Deel 2-1: Algemene eisen voor onderdelen	2000
NEN-EN 50133-7:1999	Alarmsystemen - Toegangsbewakingssystemen voor beveiligingstoepassingen - Deel 7: Richtlijnen voor de toepassing	1999
NEN-EN 2535 + A1:2002	Brandveiligheid van gebouwen - Brandmeldinstallaties - Systeem- en kwaliteitseisen en projecteringsrichtlijnen	1996 2002
NEN-EN 2575 + C1:2006	Brandveiligheid van gebouwen - Ontruimingsinstallaties - Systeem- en kwaliteitseisen en projecteringsrichtlijnen	2004 2006

Allen verkrijgbaar via www.nen.nl.



I Inbraakwerendheid

Beveiligingsniveau - risicoklasse

Indien er voor een terrein of object een bepaald beveiligingsniveau is vastgesteld, bijvoorbeeld overeenkomstig de VRKI vanuit het Handboek Beveiligingstechniek, dan zal het toegangscontrolesysteem geen nadelige invloed hebben om de bouwkundige, organisatorische en elektronische maatregelen in die bewuste klasse.

Indien de componenten van het toegangscontrolesysteem buiten het beveiligde gebied zijn gemonteerd zal sabotage moeten worden gemeld. In geen geval mogen de doorgangen (deuren) worden ontgrendeld.

Elektrisch gestuurde deurvergrendelingen

Dergelijke deurvergrendelingen worden niet beproefd op basis van de SKG methodiek.

In de NEN 5089 (paragraaf 5.2.1.1) is wel een relatie gelegd tussen de inbraakweerstandklasse vanuit de NEN-EN 12209-3:1998 ontw. (Dit is een verwijzing uit de NEN-EN 14846:2003 ontw. voor elektromagnetisch bediende sloten en sluitplaten.).

De relatietabel is als volgt:

	Weerstandsklasse Keurmerk Elektronisch Toegangsbeheer			
	Licht	Standaard	Zwaar	Extra zwaar
NEN-EN 12209	Geen relatie	3	4	7
Manuele beproeving NEN 5089	Geen relatie	3 min	5 min	10 min
VRKI	Geen relatie	B1 (voorheen Bs)	B2 (voorheen Bn)	B3 (voorheen Bz)
Observatie-gebied	Disciplinaire vergrendelingen; Elektrische sluitplaten op de dagschoot +lichte magneten met houdkracht 100 - 150 KG	Licht beveiligde vergrendelingen; elektrische sluitplaten met dagschoot blokkering + magneten met houdkracht 300 KG		
Beveiligd gebied			Standaard beveiligde vergrendelingen; o.a sluitplaten op nachtschoot, Solenoidsloten en magneten tot ca 700 KG houdkracht	Zwaar beveiligde vergrendelingen; motorsloten, meerpuntssloten en Magneten tot een houdkracht van ca 1500 KG
Vitaal gebied				High security vergrendelingen; Grendels uit de klasse zwaar beveiligd waarbij mechanische manipulatie van buitenaf wordt beschermd.



Elektrisch gestuurde deurvergrendelingen dienen derhalve te zijn voorzien van een 'klasse' aanduiding op basis van de NEN-EN 12209 of de NEN-EN 14846. Deze aanduiding is in de vorm van een cijfer tussen 1 en 7.

De NEN-EN 14846 heeft een Annex Z dus CE markering is mogelijk.

Ter informatie:

In de vernieuwde risicoklasse indeling (VRKI) vanuit het technisch beveiligingshandboek wordt Bs, Bn en Bz niet meer genoemd. De benaming is als volgt:

B1 (voorheen Bs)

B2 (voorheen Bn)

B3 (voorheen Bz)

Observatie gebied (OG)

Openbaar/publiek gebied waar disciplinaire beveiliging is gewenst. Iemand probeert binnen te komen.

Lukt dat niet dan loopt men verder.

Met grof geweld kom je wel binnen.

Beveiligd gebied (BG)

Niet openbaar/publiek gebied waar iemand die grof geweld gebruikt wordt tegengehouden.

Vitaal gebied (VG)

Gebied waar beperkte toegang is en wat essentieel is om onbevoegden te weren om het bedrijfsproces te continueren en te garanderen.

Technische uitvoering:

Binnen het certificatieschema 'Keurmerk Elektronisch Toegangsbeheer' is het van belang dat elektrisch gecontroleerde sloten en sluitplaten voldoen aan de volgende voorwaarden:

- de werking van een slot moet een bepaalde tijd wordt gegarandeerd ook bij stroom uitval (accu back-up)
- in het slot dient een functionaliteit te zitten om de status van het slot te signaleren (terugmeld contact).
- CE-markering

Voor de deur geldt dat deze zelfsluitend moet zijn doormiddel van bijvoorbeeld een deurdranger. Ook moet er een signalering op zitten wat de stand van de deur is (deurstand signalering)



II Vluchtveiligheid

Vluchtdeuren

Aan capaciteit, projectering, uitvoering en beheer van vluchtdeuren mogen geen concessies worden gedaan. Onvoorwaardelijk geldt: vluchtdeuren moeten onder alle omstandigheden zonder sleutel snel geopend kunnen worden in de vluchtrichting.

Normen

- NEN-EN 179 Sluitingen voor nooduitgangen (Emergency exit devices);
- NEN-EN 1125 Panieksluitingen (Panic exit devices).

elektrisch gestuurde panieksluitingen:

- NEN-EN 13633 Elektromechanisch gestuurde vluchtdeursluitingen (Panic exit systems);
- NEN-EN 13637 Elektromechanisch gestuurde nooddeursluitingen (Emergency exit systems).

Elektrisch gestuurde sluitingen bieden een breed scala aan mogelijkheden, waaronder het integreren in brand- en inbraakmeldsystemen, toegangscontrole- en tijdregistratiesystemen en overvalbeveiliging. Hier onderscheiden we de systemen gebaseerd op ruststroomprincipe, handbediening, centrale bediening en automatische sturing.

Ruststroomprincipe (geen spanning = ontgrendelen)

Alle elektrische deurvergrendelingen moeten functioneren volgens het zogenoemde ruststroomprincipe. Dit betekent dat de vergrendeling wordt ontgrendeld bij spanningsonderbreking. Deze eis staat vaak haaks op de eis vanuit toegangscontrole dat een deur onder geen beding mag worden ontgrendeld als de stroom wegvalt.

Handbediening (groene bedienknop met instructie)

Bij elke vergrendelde deur moet binnen 50 cm van de deurkruk een handbediening aanwezig zijn om deze deur te kunnen ontgrendelen. De bedienknop kan zijn uitgevoerd overeenkomstig een handmelder. Er dient altijd van te worden uitgegaan dat slechts één handeling nodig is om de deur te ontgrendelen. De kleur van de bedienknop dient groen te zijn. Op of in de nabijheid van deze bedienknop moet in de Nederlandse taal vermeld staan welke handeling moet worden verricht, bijvoorbeeld 'glas inslaan'.

Ook moet een tekst over het doel van de bedienknop worden aangebracht, te weten 'deurontgrendeling'. De bedienknop mag geen relatie hebben met een eventueel brandmeld- en/of gebouwbeheerssysteem.

De bedienknop moet bij voorkeur tussen de 900 en 1200 mm boven de vloer worden geïnstalleerd.

Centrale bediening (alle deuren gelijktijdig ontgrendelen)

Tevens moet, bijvoorbeeld bij een receptie, de mogelijkheid aanwezig zijn voor centrale ontgrendeling met behulp van een bedienknop.

Automatische sturing (brandmelding = ontgrendelen)

Indien in het betreffende object een brandmeld- of een ontruimingsalarminstallatie aanwezig is, moeten bij activering daarvan automatisch alle deurvergrendelingen worden ontgrendeld. Bij nood- en vluchtdeuren gaat de voorkeur uit naar elektromagnetische vergrendelingen. Elektrische sloten mogen ook worden toegepast, op voorwaarde dat een speciale schootconstructie het gemakkelijk ontgrendelen bij duwkrachten op het deurblad voldoende waarborgt. Als referentie wordt verwezen naar hoofdstuk 10 van de NVBR:2005.



III Brandveiligheid

Vanuit het Bouwbesluit heeft de brandwerendheid voor deuren / doorgangen prioriteit.

Basis wordt omschreven in de normen:

- NEN 2535 (Brandmeldinstallatie - BMI)
- NEN 2575 (Ontruimingsalarminstallatie - OAS)

Indien er naast een BMI / OAS installatie ook een toegangscontrolesysteem aanwezig is een gebouw is er een conflict met het kunnen ontgrendelen van deuren.

Vanuit een brandmeldinstallatie en/of een ontruimingsalarminstallatie mogen deuren niet worden ontgrendeld door middel van een toegangscontrolesysteem. De deuren moeten direct met een verbreekcontact tussen voeding en elektrisch slot worden ontgrendeld. (Groene knop). Resultaat: Een deur is te openen zonder tussenkomst van het toegangscontrolesysteem.

In het PvE voor Toegangscontrolesystemen dient dit aspect te zijn benoemd.



IV Modeltekst procescertificaat

De certificerende instelling dient bij de afgifte van het procescertificaat (bedrijfserkenning) de onderstaande teksten te hanteren bij het toepassingsgebied.

Bedrijfserkenning	Toepassingsgebied
Leverancier Toegangscontrolesystemen	Het leveren van componenten van een toegangscontrolesysteem onder keurmerk
Adviesbureau Toegangscontrolesystemen	Het leveren van een PvE + projectering van een toegangscontrolesysteem onder keurmerk
Technisch Toegangscontrolebedrijf	Het opstellen van het detailontwerp, het installeren en opleveren van een toegangscontrolesysteem onder keurmerk
Onderhoudsbedrijf Toegangscontrolesystemen	Het leveren van de dienst onderhoud aan een TCS onder keurmerk

Het procescertificaat dient te zijn voorzien van een uniek certificaatnummer, een ingangsdatum, een versienummer, NAW gegevens van de certificaathouders en de vestigingen van de certificaathouder die onder het certificaat vallen.

Op het certificaat zal het keurmerk zichtbaar op de voorzijde zijn afgedrukt.





V Oplevercertificaat Toegangscontrolesysteem

Oplevercertificaat Toegangscontrolesystemen

Gegevens opdrachtgever

-
-
-

Datum afgifte certificaat

Registratienummer certificaat



Locatiegegevens van het Toegangscontrolesysteem

-
-
-

Kenmerk PvE:.....

Kenmerk keurmerk productsamenstelling TCS:.....

Classificatie Toegangscontrolesysteem:

Verklaring certificerende instelling

Op grond van onderzoek, evenals regelmatig door de certificerende instelling uitgevoerde audits, worden door onderstaande certificaathouder ontworpen en aangelegde Toegangscontrolesystemen geacht te voldoen aan de eisen die gesteld zijn in de beoordelingsrichtlijn "Elektronisch Toegangsbeheer"

Verklaring Certificaathouder

De certificaathouder verklaart dat de werkzaamheden zijn uitgevoerd in overeenstemming met de voorschriften zoals zijn vastgelegd in de Beoordelingsrichtlijn "Elektronisch Toegangsbeheer" en dat het Toegangscontrolesysteem voldoet aan de eisen die daaraan gesteld worden.

Gebbruiksfase; uitgangspunten:

- Er dient jaarlijks onderhoud te worden uitgevoerd
- Er dient een opgeleid persoon te worden aangesteld voor het toegangscontrolesysteem
- Uitbreidingen / bouwkundige wijzigingen kunnen gevolgen hebben voor de correcte werking van het systeem. Neem voor advies contact op met een Adviesbureau Toegangscontrolesystemen

Wenken voor de afnemer

Bij ontvangst van het Opleverbewijs controleren of:

- De certificaathouder nog beschikt over een geldig procescertificaat;
- Het Toegangscontrolesysteem is uitgevoerd en opgeleverd volgens de afspraak;
- Het Toegangscontrolesysteem functioneert zoals het zou moeten doen;

<<Naam installatiebedrijf>>

<< Naam TBV'er >>

Handtekening

<<TBV'er>>

Indien op grond van bovenstaande of op basis van andere redenen het Toegangscontrolesysteem niet in orde wordt bevonden, dient u contact op te nemen met:

1. De certificaathouder;
2. De certificerende instelling.



VI Melden projecten

Voor het melden van een project dient de certificaathouder onderstaande gegevens door te sturen aan de CI:

AANMELDEN PROJECT

Installatie Toegangscontrolesysteem

Erkend Installateur Toegangscontrole

Bedrijfsnaam:

Contactpersoon:

Telefoonnummer contactpersoon:

Projectgegevens

Datum aanvang werk:

Datum beëindiging werk:

Projectlocatie

Adres (exacte locatie) :

Plaats :

Naam installatiedeskundige:

Telefoon installatiedeskundige op het werk:

Bijzonderheden gelet op de toegankelijkheid van de projectlocatie :

Wijzigingen of annuleringen van projecten dienen duidelijk en per omgaande aan de CI te worden gemeld.



VII Checklist Opleveren Toegangscontrolesysteem

Basismodel checklist opleveren Toegangscontrolesysteem door een Technisch Toegangscontrolebedrijf:

A - Gegevens			
Naam installateur			
Datum			
Locatie			
PvE nummer			
Tekeningnummer			
B - Oplevercontrole	akkoord	Niet akkoord	Nvt
Controle keurmerk op componenten			
Controle keurmerk op PvE en projectie			
Controle werking doorgangen; alles werkt, getest 100%			
Controle op de eisen van het transmissiesysteem			
Controle op de eisen aan opgeslagen gegevens – Wbp			
Controle tekening; de realisatie komt overeen met de tekening			
Controle op overige eisen			
C - Conclusie	Akkoord	Niet akkoord	
Het toegangscontrolesysteem voldoet aan de eisen die zijn gesteld in het PvE zoals bij A genoemd			
Datum :			
Handtekening :			



VIII Standaard PvE Toegangscontrolesysteem

Gegevens		
	Datum opmaak	:
	Documentnummer	:
Object :	Naam	:
	Adres	:
	Postcode / plaats	:
	Contactpersoon	:
	Telefoon / e-mail	:
Opdrachtgever	Naam	:
PVE – opsteller Toegangscontrole	Naam	:
	Telefoon / e-mail	:
	Werkzaam bij	:
Installateur <i>Indien reeds bekend</i>	Naam	:
Leverancier <i>Indien reeds bekend</i>	Naam	:
Eisende partij(en)	Naam	:
	Naam	:
	Naam	:



Eisen Toegangscontrolesysteem

Paragraaf uit certificatieschema

3.2	Omvang / afbakening	Aantal zones / groepen personen	:
		Aantal objecten	:
		Grootte terrein	:
		Aantal doorgangen	:
		Plaats centrale verwerkingseenheid + server	:
1.4 + 3.2	Classificatie Tabel Bijlage X Keurmerk Elektronisch Toegangsbeheer	1 /t/m 10 1 = laag 10 = hoog	:
3.1.3	Transmissie	Bedraad / raadloos	:
4.7	Opgeleid persoon	Naam:	:
3.1.4	Eisen opslag persoonsgegevens	Wet bescherming persoonsgegevens van toepassing?	:



Beheer en uitvoering		
Alarmering	Afspraak over wijze van melden	:
	Verschilende alarmen	:
	Opvolging georganiseerd	:
	Deurstandsignalering	:
	Overig	:
Funcities	Tijdregistratie	:
	Parkeerbeheer	:
	Bezoekregistratie	:
	Anti-pass back	:
	Personeelsregistratie	:
	Facturatie	:
	BHV-toepassingen	:
	overig	:
Database	Specificaties	:
Noodstroom	12 uur gangreserve	:
	Alarm (Netspanning / accu)	
	Sturingen separaat	
Integratie bestaand toegangscontrolesysteem		- <i>Zelfstandig werkende sloten en vergrendelingen zonder aansluiting op de centrale verwerkingseenheid</i>
Intrgratie CCTV systemen		- <i>Koppeling met het toegangscontrole-systeem</i>



Sturingen

Doorgangen / deuren	<ul style="list-style-type: none">- <i>Mogelijkheid tot centrale ontgrendeling, bijv. bedienknop receptie</i>- <i>Bij activering ontruimingalarminstallatie automatische ontgrendeling doorgangen.</i>
---------------------	---

Integratie overig gebouwbeheer

Inbraak	consequenties inbraakwerendheid	<ul style="list-style-type: none">- <i>Beveiligingsklasse en –maatregelen (BORG)</i>- <i>Montage componenten buiten beveiligd gebied</i>- <i>Sturing vanuit centrale verwerkingseenheid toegangscontrole op sluitmechanisme bij doorgangen?</i>
Brand	Consequenties brandveiligheid?	<ul style="list-style-type: none">- <i>Installatie conform NEN 2535</i>- <i>Ontgrendelen deuren vanuit BMC zonder tussenkomst toegangscontrolesysteem</i>
Vluchten	Consequenties vluchtveiligheid	<ul style="list-style-type: none">- <i>Elektrisch gestuurde panieksluitingen aanwezig die ook onderdeel zijn van het toegangscontrolesysteem?</i>- <i>Werking op basis van ruststroomprincipe?</i> (geen spanning= ontgrendelen)- <i>Zijn er consequenties voor de capaciteit en uitvoering van de vluchtdeuren door installatie van het toegangscontrolesysteem</i>



Goedkeuring		
Opdrachtgever	Naam: Contactpersoon:	Datum: Handtekening
PVE-opsteller	Naam: Contactpersoon:	Datum: Handtekening
Eisende partij(en)	Naam: Contactpersoon:	Datum: Handtekening
	Naam: Contactpersoon:	Datum: Handtekening

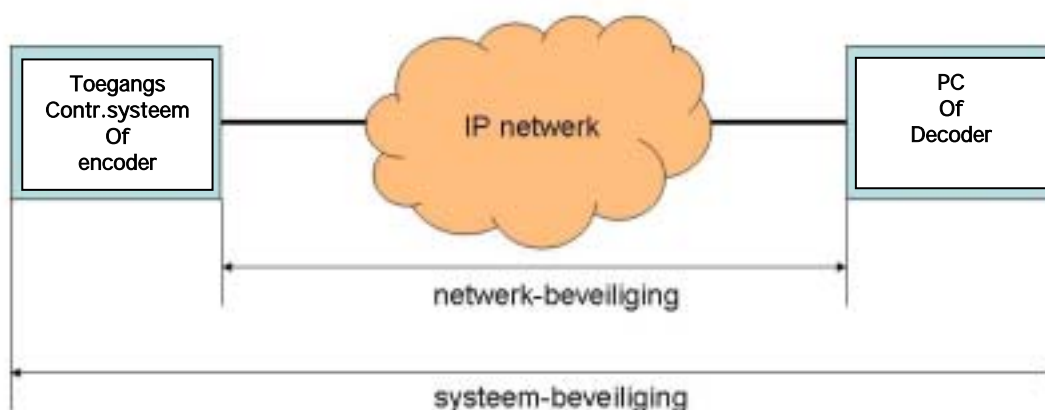
IX Beveiligingsprotocol transmissie

Inleiding

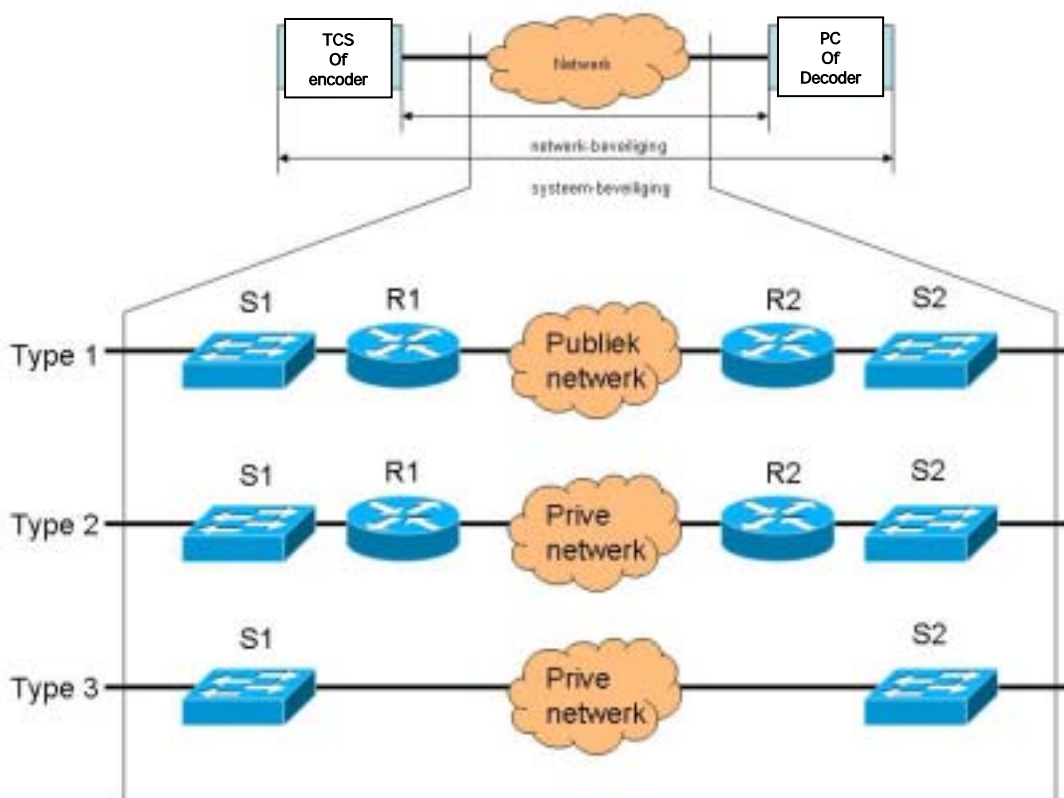
Een onderdeel van deze beoordelingsrichtlijn is beveiliging van de transmissiewegen. De beoordelingsrichtlijn is bedoeld voor zowel analoge als digitale systemen. In dit document zal worden ingegaan op uitsluitend beveiliging van digitale systemen (lees IP-systemen). Hierbij zal intensief gebruik gemaakt worden van standaarden op dit gebied.

Beveiligen van een digitaal systeem

Om het transmissiepad van een digitaal systeem te beveiligen, is eerst inzicht nodig in tot hoever de beveiliging kan strekken en welk type netwerken er zijn. Beveiliging van het transmissie pad kan volledig worden overgelaten aan de aangesloten systemen, de zogenaamde *stelsysteem-beveiliging*. De beveiliging begint en eindigt op de aangesloten apparatuur. Voorwaarde hierbij is dat de apparatuur hier voorzieningen heeft getroffen, om dit aan te kunnen. In de praktijk is dit niet altijd het geval, waardoor men is aangewezen op *netwerk-beveiliging*.



Netwerk-beveiliging loopt van aansluiting (poort) tot aansluiting. Het systeem is hier buiten gelaten. Dit is in de praktijk de meest voorkomende manier van beveiligen. Het netwerk is op een aantal manieren in te richten. Per inrichting komen er verschillende aspecten naar voren, waar de beveiliging op afgestemd moet worden. De typen netwerken zijn weergegeven in tekening 2.



- **Type 1**
De uiteinden van het transmissie pad zijn voorzien van switches (S1 & S2). Deze zijn gekoppeld aan routers (R1 & R2). De routers zijn vervolgens gekoppeld via een publiek netwerk (Internet, netwerk van dienstverlener). Dit type netwerk wordt veelal gebruikt om grotere afstanden te overbruggen.
- **Type 2**
De opbouw is identiek aan type 1, echter het publieke netwerk heeft plaatsgemaakt voor een prive netwerk. Dit type netwerk wordt veelal gebruikt tussen lokaties die op korte afstand van elkaar staan.
- **Type 3**
Hierbij zijn switches S1 & S2 via een prive netwerk aan elkaar gekoppeld. Dit type netwerk is veelal te vinden in een pand.



Het beveiligen van een systeem dat gebruik maakt het IP-protocol dient vijf aspecten te dekken, te weten:

1. *Authenticatie*; controle dat alleen geauthenticeerde entiteiten toegang krijgen tot het netwerk.
2. *Authorisatie*; bepalen wat de geauthenticeerde entiteit mag doen na verleende toegang
3. *Confidentialiteit van data door middel van encryptie*; het onleesbaar maken van informatie voor niet geauthenticeerde gebruikers
4. *Integriteit van data*; het authenticeren door de ontvanger van data die door de zender zijn verstuurd, zodat er geen data-manipulatie geweest kan zijn in het transmissiepad.
5. *Detectie van herhaalde pakketten*; Pakketten die gecopiëerd zijn en vervolgens herhaald worden verstuurd, dienen te worden gedetecteerd en geblokkeerd.

De vijf aspecten worden hieronder verder uitgewerkt, waarbij aangegeven wordt welke technieken er gebruikt kunnen worden en hoe de werking ervan aantoonbaar gemaakt kan worden.

1. Authenticatie

Doel: controle dat alleen geauthenticeerde entiteiten toegang krijgen tot het netwerk.

Hoe te realiseren:

- MAC- en/of IP-adres filtering op koppelvlak activeren
- Maximaal 1 entiteit per koppelvlak toelaten en deze fixeren
- Bij een poging tot toegang verkrijgen met een niet-geauthenticeerd apparaat dient een SNMP Trap-melding gegenereerd te worden en opgevolgd te worden door een network management systeem of relevante applicatie.

Hoe dit aantoonbaar te maken:

- Het testen van de verbinding van door middel van een ICMP echo-request en echo-reply (ook wel 'ping' genoemd). Dit conform RFC792 (IPv4) of RFC2493 (IPv6). De verbinding moet blokkeren als een niet-geauthenticeerd apparaat is aangekoppeld en doorgang verlenen als het geauthenticeerd apparaat is aangekoppeld.
- Het netwerk-apparaat waaraan het apparaat aan gekoppeld is, dient met behulp van overzichtslijsten aan te tonen dat alleen het geauthenticeerde MAC- of IP-adres toegelaten wordt.

2. Authorisatie

Doel: Bepalen wat de geauthenticeerde entiteit mag doen na verleende toegang.

Hoe te realiseren:

- Implementeren van IP-filters in routers en L3-switches.
- Implementeren van VLAN's (Virtual LAN's) in L2-switches, waarin alleen apparatuur in geplaatst wordt die met elkaar moeten communiceren.
- [optioneel] Implementeren van filters ten behoeve van inter-VLAN verkeer

Hoe dit aantoonbaar te maken:

- Het testen van de verbinding van door middel van een ICMP echo-request en echo-reply (ook wel 'ping' genoemd). Dit conform RFC792 (IPv4) of RFC2493 (IPv6). De verbinding moet blokkeren als een geauthenticeerd apparaat met een niet toegestane ontvangende apparaat communiceert en doorgang verlenen als een geauthenticeerd apparaat communiceert met een toegestane ontvangende apparaat communiceert.



-
- Het netwerk-apparaat waaraan het apparaat aan gekoppeld is, dient met behulp van overzichtslijsten aan te tonen dat alleen een geauthenticeerde apparaat mag communiceren met toegestane ontvangende apparatuur.

3. Confidentialiteit van data door middel van encryptie

Doel: Het onleesbaar maken van informatie voor niet geauthenticeerde gebruikers.

Hoe te realiseren:

- Voor situaties 1 en 2 het inzetten van IPsec, conform de geldende RFC's
- [optioneel] Voor situatie 3 is Secure-HTTP conform RFC2660 mogelijk voor aangesloten apparaten die dit ondersteunen.

Hoe dit aantoonbaar te maken:

- Het netwerk-apparaat (router) waaraan het apparaat aan gekoppeld is, dient met behulp van overzichtslijsten aan te tonen dat de verbinding tussen zender en ontvanger versleuteld is.
- [optioneel] Het aangesloten apparaat, dient met behulp van overzichtslijsten aan te tonen dat alleen een geauthenticeerde apparaat mag communiceren met toegestane ontvangende apparatuur.

4. Integriteit van data

Doel: Het authenticeren door de ontvanger van data die door de zender zijn verstuurd, zodat er geen data-manipulatie geweest kan zijn in het transmissiepad.

Hoe te realiseren:

- Voor situaties 1 en 2 het inzetten van IPsec, conform de geldende RFC's

Hoe dit aantoonbaar te maken:

- Het netwerk-apparaat, dient met behulp van overzichtslijsten aan te tonen dat alleen een geauthenticeerde apparaat mag communiceren met toegestane ontvangende apparatuur.

5. Detectie van herhaalde pakketten

Doel: Pakketten die gekopieerd zijn en vervolgens herhaald worden verstuurd, dienen te worden gedetecteerd en geblokkeerd.

Hoe te realiseren:

- Voor situaties 1 en 2 het inzetten van IPsec, conform de geldende RFC's

Hoe dit aantoonbaar te maken:

- Het netwerk-apparaat, dient met behulp van overzichtslijsten aan te tonen dat alleen een geauthenticeerde apparaat mag communiceren met toegestane ontvangende apparatuur.



Beveiligen van IP-infrastructuur tegen wijzigingen door niet geautoriseerde beheerders

Om hier tegen te kunnen beveiligen zijn er twee methoden beschikbaar:

- Over de aanwezige IP-infrastructuur wordt een extra beveiligingslaag met Laag 3 routers gebouwd op basis van IPsec. Deze componenten (en daarmee de beveiliging) worden beheerd door de installateur.
- Beveiliging door middel van rol-gebaseerd beheer. De Laag 3 routers dienen verschillende rollen te erkennen, waarbij een rol weggelegd is voor de netwerkbeheerder t.b.v. operationeel infrastructuurbeheer en een rol voor de installateur om de beveiliging te kunnen regelen.



X Classificatie

Voor de classificatie per doorgang wordt gebruik gemaakt van onderstaande tabellen.

Klasse	Definitie	Toepassing	Organisatorische aanvulling	Identificatie principe
1	Identificatie middel zonder versleuteling van gegevens en welke zonder hulpmiddelen of vaardigheden kan worden gereproduceerd.	Als eenmalige toegangspas voor locaties welke geclassificeerd worden als zeer laag risico.	Toegangspassen dient na eenmalige toegangsverlening te worden geblokkeerd.	Pincode Barcode Barcode met IR strip
2	Identificatie middel zonder versleuteling van de gegevens en welke met beperkte hulpmiddelen gereproduceerd kan worden zonder specifieke vaardigheden.	Als reguliere toegangspas voor objecten met de classificatie laag risico.		Magneetstrip
3	Identificatie middel zonder versleuteling van de gegevens en welke met beperkte hulpmiddelen en specifieke vaardigheden gereproduceerd kan worden.	Als reguliere toegangspas voor objecten met de classificatie laag en middelhoog risico.		Wiegand Proximity (no encryptie) CS nummer smart prox
4	Identificatie middel met versleuteling van de gegevens en welke met beperkte hulpmiddelen en specifieke vaardigheden gereproduceerd kan worden.	Als reguliere toegangspas voor ruimten met de classificatie hoog risico binnen objecten met een laag en middelhoog risico.		Proximity (met beperkte encryptie)
5	Identificatie middel zonder versleuteling van de gegevens en welke met beperkte hulpmiddelen en specifieke vaardigheden gereproduceerd kan worden. Gecombineerd met pincode of biometrische verificatie.	Als reguliere toegangspas voor objecten met de classificatie middelhoog risico.	Toegangspas en pincode/biometrie dienen in het systeem te worden gekoppeld voor toegangsverlening.	Wiegand Proximity (no encryptie) CS nummer smart prox
6	Identificatie middel met versleuteling van de gegevens en welke met uitgebreide hulpmiddelen en specifieke vaardigheden gereproduceerd kan	Als reguliere toegangspas voor ruimten met de classificatie hoog risico binnen objecten met een middelhoog risico.		Proximity (met complexe encryptie)



Klasse	Definitie	Toepassing	Organisatorische aanvulling	Identificatie principe
	worden.			
7	Identificatie middel met versleuteling van de gegevens en welke met beperkte hulpmiddelen en specifieke vaardigheden gereproduceerd kan worden. Gecombineerd met pincode of biometrische verificatie.	Als reguliere toegangspas voor objecten met de classificatie hoog risico.	Toegangspas en pincode/biometrie dienen in het systeem te worden gekoppeld voor toegangsverlening. Pincode of biometrische gegevens mogen niet op de kaart worden opgeslagen.	Proximity (met beperkte encryptie)
8	Identificatie middel met versleuteling van de gegevens en welke met uitgebreide hulpmiddelen en specifieke vaardigheden gereproduceerd kan worden. Gecombineerd met pincode of biometrische verificatie.	Als reguliere toegangspas voor ruimten met de classificatie zeer hoog risico binnen objecten met een hoog risico.	Toegangspas en pincode/biometrie dienen in het systeem te worden gekoppeld voor toegangsverlening. Pincode of biometrische gegevens mogen niet op de kaart worden opgeslagen.	Proximity (met complexe encryptie)
9	Identificatie middel met versleuteling van de gegevens waarvan op basis van de huidige kennis mag worden uitgegaan dat het reproduceren ervan praktisch is uitgesloten.	Als reguliere toegangspas voor objecten met de classificatie zeer hoog risico.	De buitenschil dient minimaal te worden beschermd overeenkomstig klasse 10.	Conform FIPS 201
10	Identificatie middel met versleuteling van de gegevens waarvan op basis van de huidige kennis mag worden uitgegaan dat het reproduceren ervan praktisch is uitgesloten. Gecombineerd met pincode of biometrische verificatie.	Als reguliere toegangspas voor de buitenschil van objecten met de classificatie zeer hoog risico.	Toegangspas en pincode/biometrie dienen in het systeem te worden gekoppeld voor toegangsverlening. Pincode of biometrische gegevens mogen niet op de kaart worden opgeslagen.	Conform FIPS 201



Klasse	<i>Uitvoering leeskop</i>	<i>Deursturing</i>
1	Lezer zonder encryptie waarbij alle technologie is ondergebracht in de kaartleeskop.	In de kaartleeskop aan de niet beveiligde zijde van de toegang.
2	Lezer met of zonder encryptie waarbij de kaartlezer middels een niet gecodeerd communicatie signaal (Wiegand/Omron) is verbonden met een deurbesturing unit.	In de deurbesturing unit welke is geplaatst aan de beveiligde zijde van de toegang.
3	Lezer met of zonder encryptie waarbij de kaartlezer middels een niet gecodeerd communicatie signaal (Wiegand/Omron) is verbonden met een deurbesturing unit. Afnemen van de lezer wordt gesignaleerd als alarmmelding waarna de deursturing wordt geblokkeerd.	In de deurbesturing unit welke is geplaatst aan de beveiligde zijde van de toegang.
4	Lezer zonder encryptie waarbij de kaartlezer middels een gecodeerd communicatie signaal is verbonden met een deursturing unit.	In de deurbesturing unit welke is geplaatst aan de beveiligde zijde van de toegang.
5	Lezer met encryptie waarbij de kaartlezer middels een gecodeerd communicatie signaal is verbonden met een deursturing unit. Versleuteling tussen kaart en kaartlezer en tussen kaartlezer en	In de deurbesturing unit welke is geplaatst aan de beveiligde zijde van de toegang.

*Algemene bemerking voor alle klassen:

- De lezer dient de volledige data inhoud te lezen en te verwerken in het bovenliggend systeem. Classificatie geldt niet voor die producten welke slechts een deel van de data verwerken.



XI Zonering Toegangscontrolegebied

Indien van toepassing vallen buitengebieden (veelal openbare ruimtes) op basis van dit certificatieschema ook onder het toegangscontrolegebied.

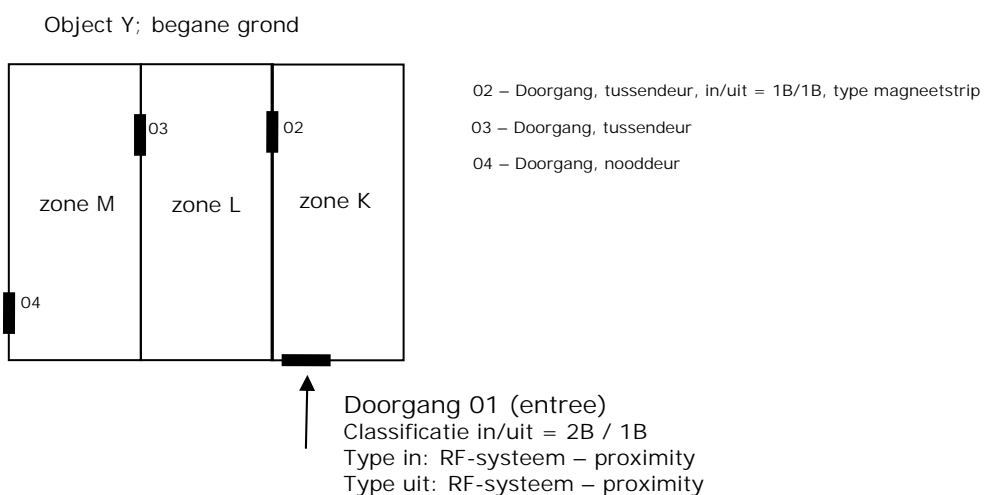
Indien het alleen om een object gaat (gebouw) dan is er geen buitengebied.

Het gebied dat net buiten het toegangscontrolegebied valt wordt ook wel de buitenschil genoemd. Alles binnen het gebied de binnenschil. Verder worden de begrippen observatiegebied, vitaal gebied en beveiligd gebied bij voorkeur toegepast.

De objecten die binnen het toegangscontrolegebied staan zijn – per object - vervolgens weer de zoneren. (minimaal 1 zone is altijd aanwezig).

De uitwerking is veelal op basis van een 'ruimte indeling' waarbij voor detaillering gebruik wordt gemaakt van bouwtekeningen met een horizontale projectie.

Onderstaand een voorbeeld van een opzet van een projectie. Bekabeling, plaats paslezers etc is niet bepaald in dit voorbeeld.





XII Onderhoudsrapport

Basismodel onderhoudsrapport Toegangscontrolesysteem:

A - Gegevens	
Naam Onderhoudsbedrijf	
Datum uitvoer onderhoud	
Locatie	
PvE kenmerk	
Projectie kenmerk	
Detailontwerp kenmerk	

B – Onderhoud	akkoord	Niet akkoord	Nvt
Controle werking doorgangen; alles werkt, getest 100%			
Controle tekening; de huidige installatie komt overeen met de tekening			

C – Reparatie	akkoord	Niet akkoord	Nvt
Afwijkingen gerepareerd; alleen componenten vervangen; doorgang(en) positief getest			
	-		
	-		
	-		

D – Reparatie	Component	Locatie
Vervangen componenten:	-	-
	-	-
	-	-

E – Conclusie	Akkoord	Niet akkoord
Het toegangscontrolesysteem is onderhouden conform aan de eisen die zijn gesteld in de het certificatieschema Keurmerk Elektronisch Toegangsbeheer		Neem contact op met een Adviesbureau Toegangscontrolesystemen.
Datum :		
Handtekening :		



XIII Specificatieblad geïntegreerde productsamenstelling

A – Gegevens Leverancier Toegangscontrole	
Naam	
Certificaatnummer	

B – Merk en type Toegangscontrolesysteem	
Merk	
Type	

C - Componenten	Omschrijving

D - Conclusie	Akkoord	Niet akkoord
De geïntegreerde productsamenstelling voldoet aan de eisen die zijn gesteld in het certificatieschema Keurmerk Elektronisch Toegangsbeheer.		
Datum validatie :		
Handtekening :		