

Paxton Specificatie

Sectie 6

Paxton10 Lezers

Bewerk dit document indien nodig - dit document kan worden gebruikt voor een standalone Entry deurintercom systeem, of waar nodig worden samengevoegd met een Paxton online op maat gemaakte toegangscontroleoplossing.

**[Vierkante haakjes]:** Standaard -– Opties.
**{Krulhaken}:** Opmerkingen

SECTIE 6

TOEGANGSCONTROLE – Paxton10

**1.1 SAMENVATTING**

1. Sectie bevat:
	1. Toegangscontrole en videomanagement
2. Gerelateerde onderdelen
	1. 28 10 00 Toegangscontrole en Videomanagement
	2. 28 13 00 Toegangscontrole
3. Producten

(Verwijder indien niet benodigd voor het project)

(Kies bij elk van de regels hieronder voor de Paxon productnaam of een algemene benaming.

* 1. Een [proximity lezer] [Paxton10 lezer], welke meerdere kaartdataformaten leest, inclusief Bluetooth, om gebruikers te verifieren en toegang te verlenen.
	2. Een [vandaalbestendige proximity lezer] [Paxton10 VB lezer], welke meerdere kaartdataformaten leest, inclusief Bluetooth, om gebruikers te verifieren en toegang te verlenen met een lezer in een vandaalbestendige behuizing.
	3. Een [keypad proximity lezer] [Paxton10 Keypad lezer], welke meerdere kaartdataformaten leest, inclusief Bluetooth en de mogelijkheid om gebruik te maken van codes en PIN's om gebruikers te verifieren en toegang te verlenen.
	4. Een [desktop lezer] [Paxton10 Desktop lezer], welke de mogelijkheid biedt elektronische kaarten en tags, ook wel credentials genoemd, te programmeren in het systeem en deze te koppelen aan gebruikers.
1. Systeem
	1. De lezers zijn een fundamenteel onderdeel van het toegangscontrole systeem welke controle en inzage bieden bij de tegenpunten op een locatie of gebouw.
	2. Het systeem is schaalbaar en laat het toe het systeem verder uit te breiden met meerdere lezers [en overige toegangscontrole hardware] van dezelfde fabrikant.
	3. De lezers zijn plug-and-play.
	4. (Verwijder indien nodig hieronder de regels welke niet van toepassing zijn voor het project)
	5. Het systeem bevat meerdere toegangspunten.
	6. Het systeem bevat meerdere aan te sturen apparaten.
	7. Het systeem bevat meerdere te monitoren apparaten.
	8. Het systeem bevat inbraak- en brandalarm.
	9. Het systeem bevat videobewaking camera's.

**1.2. PROJECT VEREISTEN**{Verwijder/wijzig alles wat niet van toepassing is op dit project}

1. Een lezer zal naast ieder toegangspunt geplaatst worden op locatie om deze toegang te kunnen beveiligen en te controleren.
2. Lezers worden geplaatst bij de ingang en uitgang van een gebied voor toepassing van anti-passback.
3. Aan iedere gebruiker zal een credential worden uitgegeven.
	1. Het geïnstalleerde systeem ondersteunt minimaal 50.000 unieke credentials.
4. Een lezer wordt geplaatst voor het in- en uitschakelen van een inbraakalarm systeem.
5. Lezers worden met één kabel aangesloten welke de voeding én de communicatie naar de lezer verzorgt.
6. De lezers welke toegepast worden zullen voldoen aan de eisen welke gesteld zijn voor de toegangscontrole op het project.
7. {Verwijder indien nodig} De lezers worden geplaatst op een locatie waar alreeds een [Paxton10] systeem geïnstalleerd is.
8. {Verwijder indien nodig} De lezers worden geplaatst met overige [Paxton10] hardware and software om in een compleet toegangscontrole systeem te kunnen voorzien.
9. Lezer mogelijkheden
	1. De lezers ondersteunt de mogelijkheid om gebruikers te identificeren.
	2. Iedere lezer ondersteunt de mogelijkheid om de data van de aangeboden credential te communiceren naar een controller.
	3. Het systeem ondersteunt 2 lezers welke aangesloten kunnen worden op één controller.
	4. Lezers geven een terugkoppeling van een toegang- weigering of verlening van de aangeboden credential.
10. Onderdelen van de lezers:
	1. De lezers, welke de credentials van de gebruiker kenbaar maken aan het systeem.
	2. De controllers, welke de verwerking verzorgt van het weigeren of verlenen van toegang van de gebruikers.
11. Systeem mogelijkheden
	1. Het systeem ondersteunt het beveiligen en controleren van toegang tot een locatie via elektronische controllers, kaartlezers, keypads en smartphones. De controllers worden via 230 VAC of een POE+ (at) voeding gevoed en worden toegepast binnen een TCP/IP netwerk infrastructuur.
	2. Het systeem ondersteunt het monitoren van alarmen, het aansturen van apparaten/deuren en het maken van liftsturingen voor verschillende verdiepingen
	3. Het systeem ondersteunt het starten vanaf één enkele deur en de mogelijkheid voor het uitbreiden per deur tot een maximum van in totaal 1000 deuren.
	4. Op elke controller kan de noodzakelijke hardware worden aangesloten om een deur te beveiligen. Wanneer ingaande en uitgaande beveiliging is vereist wordt dit ondersteunt door één deurcontroller.
	5. Elke controller bevat de complete database informatie om ervoor te zorgen dat wanneer deze niet meer verbonden is met het systeem, offline door blijft functioneren.
	6. De controllers gebruiken IPv6 techniek welke zorgen voor een plug-and-play systeem met automatische detectie van de controllers.
	7. Het systeem ondersteunt ongelimiteerde toegang vanaf verschillende werkstations voor het programmeren en beheren van het systeem, inclusief database beheer, rapportage functies en het inzien van real-time gebeurtenissen
	8. Er zijn geen licenties nodig of kosten verbonden aan het gebruik van de beheer software van het systeem. Er is geen software-installatie noodzakelijk op een server of PC.
	9. Het systeem ondersteunt minimaal 50.000 unieke credentials.
12. Het systeem voorziet minimaal in het volgende:
	1. Toegangscontrole
	2. Deur status (Deur geforceerd, deur te lang open)
	3. Camerabewaking
	4. Videomanagement
	5. Gebeurtenissen rapportage
	6. Plattegronden
	7. Triggers en Acties
	8. Anti- passback
	9. Inbraakalarm integratie
	10. Brandalarm integratie
	11. Roll-Call en aanwezigheid rapportage
	12. Toegang op afstand
	13. Smartphone app voor het beheer van het systeem
	14. Smartphone app voor het beheer van de gebruikers
	15. Een lezer voor het inleren van credentials in het systeem
	16. Verschillende kaart dataformaten en bluetooth
	17. Licentievrije software en levenslange systeem updates zonder kosten
	18. Audio/video intercomsysteem
	19. Draadloze deurbeslagen

1.3 DEFENITIES

1. ABS: Acrylonitrile butadiene styrene – a thermoplastic polymer.
2. Anti-passback: Wordt gebruikt om het gebruik van doorgegeven credentials tegen te gaan zodat onbevoegde personen geen toegang kunnen krijgen tot de locatie.
3. AWG (American Wire Gauge): Een meeteenheid voor de diameter van draden.
4. Browser: Een computerprogramma dat gebruikt wordt om websites mee te bekijken.
5. Client: Een device waarmee het toegangscontrole systeem beheerd kan worden
6. COM (Common): Een contact van een relais
7. Controller: Een intelligente besturingseenheid die gebruikt wordt om de toegang te controleren en monitoren.
8. DDR3 (Double Data Rate typ 3): Het type RAM met een hoge bandbreedte.
9. Apparaat: Een camera, lamp, alarm, toegangspunt of ander stuk hardware die via de software gemonitord of aangestuurd kan worden.
10. Edge storage: Een methode waarbij de videobeelden op de camera worden opgeslagen
11. EMC: Electromagnetic Compatibility
12. Intercomsysteem: Een deurintercomsysteem dat of standalone kan functioneren of in combinatie met een toegangscontrole systeem. En wordt gebruikt om met bezoekers te communiceren door middel van audio en video.
13. FCC: Federal Communications Commission
14. I/O: Input/Output. Een input wordt gebruikt voor het monitoren van een contact of sensor. Een output is een relais waarmee een apparaat in- of uitgeschakeld worden.
15. IC: Industry Canada.
16. IP: Internet Protocol
17. LAN: Local area network.
18. Mbps: Megabits per second
19. Binnenpost: Hardware waarmee de oproep van een intercomsysteem ontvangen kan worden zodat het mogelijk is om met een bezoeker te communiceren.
20. N.C. (Normally Closed): Het verbreekcontact op een relais
21. N.O. (Normally Open): Het maakcontact op een relais
22. Bewoner/gebruiker: De gebruiker van de binnenpost
23. Open zicht: Zonder obstakels of interferentie.
24. Buitenpost: Hardware die bij een toegangspunt wordt geplaatst waarmee het voor een bezoeker mogelijk is om contact op te nemen met de bewoner van een locatie
25. PC: Personal computer: Wordt gebruikt als een werkstation om de software mee te gebruiken
26. PoE: Power over Ethernet
27. RAM (Random Access Memory): Een geheugen module die wordt gebruikt om tijdelijk informatie op te slaan. Deze informatie dient snel beschikbaar te zijn en zorgt voor een vloeiende werking van de software of besturingssysteem
28. Reader: Hardware die aangesloten wordt op een deurcontroller waarmee een gebruiker geïdentificeerd kan worden om toegang te krijgen tot een deur.
29. RoHS: Restriction of Hazardous Substances.
30. Aanwezigheidsrapporten: Een overzicht van gebruikers die op de locatie aanwezig zijn.
31. RS-485: Een TIA/EIA communicatie standaard voor seriële communicatie
32. RSS-210: IC standard for Licence-exempt Radio Apparatus.
33. RSS-GEN: IC standard for General Requirements and Information for the Certification of Radio Apparatus.
34. Software controller: Hardware dat de software en database van het systeem bevat.
35. SIP: Session Initiation Protocol.
36. Solid State Drive (SSD): Een opslag apparaat dat gebruikt van flash geheugen.
37. Systeem: De te installeren hardware en software, gecombineerd met eventuele bestaande hardware en software, om aan de eisen van het project te voldoen.
38. TCP: Transport Control Protocol
39. Credential: Een identificatie methode voor een gebruiker. Dit kan een PIN, kaart of tag zijn. Hiermee wordt bepaald of een gebruiker toegang krijgt tot de deur.
40. Triggers en acties: Een softwarefunctie waarmee regels gemaakt kunnen worden om extra sturingen aan het systeem toe te voegen.
41. UDP: User Datagram Protocol
42. UL: Underwriters Laboratories
43. Unicast: Een communicatieprotocol waarbij informatie naar één ontvanger gestuurd wordt
44. UPS: Uninterruptibe power supply
45. USB: Universal Serial Bus. Een communicatiepoort die gebruikt wordt op meeste computers
46. Vandaalbestendig (VB): Geeft aan of een product bestemd is tegen vandalisme.
47. Bezoeker: Een onbekende gebruiker die op de locatie op bezoek komt
48. WAN: Wide area network.

1.4 SYSTEEM OMSCHRIJVING

1. Algemeen
	1. Het systeem beheert de toegang van de gebruikers door de deuren op de locatie.
	2. Het systeem beheert het opnemen van videobeelden via IP-camera’s op locatie.
	3. Gebruikers worden geïdentificeerd in het systeem op basis van de volgende punten:
		1. Het aanbieden van een credential aan een lezer
		2. Het aanbieden van een smartphone, smartwatch of tablet aan de lezer
		3. Het intoetsen van een unieke pincode op een keypad
		4. Een audio of visuele bevestiging van de aanwezigheid van een gebruiker
		5. Een combinatie van het bovenstaande
	4. Het systeem dwingt het gebruik van facility of site codes met credentials niet af. Elke credential heeft een unieke encryptie voor hoge veiligheid.
	5. Het systeem voorziet in unieke kaartserienummers zodat de beheerder niet hoeft bij te houden welke kaartnummers er aangeschaft dienen te worden.
	6. Een PC, laptop of tablet wordt gebruikt om het toegangscontrole systeem te beheren.
		1. Een wachtwoord is benodigd om in het systeem in te loggen en de softwarerechten van de beheerders kunnen worden beperkt.
	7. Mobiele apps zijn beschikbaar voor systeem controle en gebruikersbeheer.
	8. De mobiele apps zijn beschikbaar voor Android en IOS-apparaten.
2. Hardware
	* 1. De hardware bestaat uit:
			1. Een software controller
			2. Deurcontrollers
			3. Videocontrollers
			4. Videocamera’s
			5. Alarm connectors
			6. Wireless connectors (benodigd voor de PaxLock)
			7. Proximity lezers
			8. Keypads lezers
			9. Desktop lezers
			10. Voedingen
		2. Alle hardware is plug and play.
		3. Alle hardware is duidelijk voorzien van labels voor een eenvoudige installatie.
		4. Alle hardware zal door de fabrikant ondersteund worden met gratis firmware updates.
3. Software
	1. De database welke alle hardware en gebruikers informatie bevat staat opgeslagen op de software controller.
	2. De software controller zorgt via een weblink voor toegang tot het systeem en de configuratie hiervan.
		1. Zonder installatie geeft het systeem op een ongelimiteerd aantal werkstations toegang tot de software.
		2. Toegang tot de software wordt gegeven met de laatst beschikbare versies van de volgende webbrowsers:
			1. Google Chrome
			2. Apple Safari
	3. Toegang tot de software wordt gegeven na het inloggen met een wachtwoord van een beheerder.
	4. De verschillende software rechten kunnen worden bepaald op basis van de verantwoordelijkheid en behoeften van de beheerders.
	5. De software zal de volgende functies bevatten:
		1. Een grafische gebruikersinterface
		2. Tooltips voor meer informatie zijn beschikbaar bij alle onderdelen.
		3. Ondersteuning voor mobiele, tablet en desktop apparaten.
		4. Meerdere gebruikers kunnen tegelijkertijd en onafhankelijk van elkaar in het systeem gebeurtenissen inzien en aanpassingen maken.
4. Functies
	1. Het systeem en de bijbehorende software zal minimaal zorgen voor het volgende functies:
		1. Toegangscontrole
		2. Video opname en videomanagement
		3. 3rd party IP camera integratie
		4. PTZ-camera ondersteuning
		5. Video wall
		6. Video exporteren
		7. Video snapshot exporteren
		8. Video bookmarks
		9. Smart search
		10. Video scrubbing
		11. Aanpassen snelheid afspelen video
		12. Inbraakalarm integratie
		13. Brandalarm integratie
		14. Gebruikers importeren
		15. Plattegronden
		16. Personaliseerbare Dashboards
		17. Favorietenbalk voor de gebruiker
		18. Automatische gebruikersverificatie in de software bij een kaartaanbieding
		19. Aanwezigheidsrapporten
		20. Aanwezigheidsrapporten email functie
		21. Aanwezigheidsrapporten op Smartphone
		22. Triggers en Acties voor personaliseerbare functies in het systeem
		23. Anti-passback
		24. Geavanceerde beheerders bevoegdheden
		25. Multiformat techniek in lezer, inclusief Bluetooth
		26. Beheer op afstand van het systeem
		27. Android en IOS mobiele apps voor het systeembeheer
		28. Android en IOS mobiele apps voor identificatie bij een lezer (Smart credential)
		29. Https-ondersteuning voor een beveiligde toegang tot de software
		30. Mogelijkheid tot het beheren en verwijderen gebruikers gebeurtenissen
		31. Software in meerdere talen beschikbaar
	2. Deze functies zijn beschikbaar zonder bijkomende kosten of abonnementen

1.5 PRESTATIE-EISEN

1. Elke wijziging die in de software wordt aangebracht, wordt automatisch doorgegeven aan alle intelligente toegangscontrole hardware, waarbij de toepasselijke wijzigingen onmiddellijk van kracht worden.
2. Gedistribueerde verwerking:
	1. Het systeem moet een volledig gedistribueerd verwerkingssysteem zijn, zodat informatie (inclusief tijd, datum, geldige codes, toegangsniveaus en soortgelijke gegevens) op zodanige wijze naar de controller wordt gedownload dat deze zelf de beslissingen neemt over de toegangscontrole voor die locatie.
	2. Als de communicatie met de server verloren gaat, bufferen alle controllers automatisch gebeurtenissen totdat de communicatie is hersteld, waarna de gebufferde gebeurtenissen naar de server worden geüpload.
3. Systeemcapaciteiten:
	1. Het systeem ondersteunt minimaal:
		1. 1.000 toegangspunten.
		2. 1.000 videocamera's.
		3. 50.000 gebruikers, elk met een unieke credential.
		4. Onbeperkte toegangsniveaus en regels.
		5. Onbeperkte rapportage

1.6 KWALITEITSBORGING

1. De gebruikte lezers krijgen gratis firmware-upgrades van de fabrikant.
2. Lezers hebben een fabrieksgarantie van minimaal 5 jaar. De volgende onderdelen vallen hieronder:
3. Elektrisch
4. Elektronisch
5. Behuizing
6. Mechanisch
7. De systeemleverancier biedt een garantie van vijf jaar op alle componenten van de lezer en zorgt voor gratis software en firmware-upgrades.

1.7   GERELATEERDE DOCUMENTEN

1. Het systeem moet communiceren met andere fysieke delen van de faciliteit en met elke constructie, zowel nieuw als gerenoveerd.
2. Bij het bepalen van locaties voor plaatsing van hardware moet de installateur alle toepasselijke bouwvoorschriften en wetten met betrekking tot veiligheid en constructie volgen.

1.8 COMPLIANCE

1. Het systeem moet voldoen aan:
	1. De Algemene Verordening Gegevensbescherming (AVG) 2018
	2. EN60839-11-1 Klasse 1
	3. EN60839-11-1 Klasse 2
2. [Proximity-lezers] [Paxton10-lezers] moeten voldoen aan de volgende normen:
	1. EN 301 489-1 voor EMC {EU}
	2. EN 300 330 voor radio {EU}
	3. EN 60950-1 voor veiligheid {EU}
	4. IEC/EN 60950-1 voor veiligheid {ROW}
	5. FCC deel 15C voor radio {US}
	6. UL294 voor veiligheid {VS}
	7. RSS-GEN, 210 voor radio {Canada}
	8. CS C22.2 NR. 205-M1983 voor veiligheid {Canada}
	9. IP67 voor vochtbestendigheid
3. [Keypads [Paxton10 keypads] moeten voldoen aan de volgende normen:
	1. EN 301 489-1 voor EMC {EU}
	2. EN 300 330 voor radio {EU}
	3. EN 60950-1 voor veiligheid {EU}
	4. IEC/EN 60950-1 voor veiligheid {ROW}
	5. FCC deel 15C voor radio {US}
	6. UL294 voor veiligheid {VS}
	7. RSS-GEN, 210 voor radio {Canada}
	8. CS C22.2 NR. 205-M1983 voor veiligheid {Canada}
	9. IP67 voor vochtbestendigheid
	10. IK10 voor slagvastheid
4. [Vandalismebestendige lezers] [Paxton10 VR-lezers] moeten voldoen aan de volgende normen:
	1. EN 301 489-1 voor EMC {EU}
	2. EN 300 330 voor radio {EU}
	3. EN 60950-1 voor veiligheid {EU}
	4. IEC/EN 60950-1 voor veiligheid {ROW}
	5. FCC deel 15C voor radio {US}
	6. UL294 voor veiligheid {VS}
	7. RSS-GEN, 210 voor radio {Canada}
	8. CS C22.2 NR. 205-M1983 voor veiligheid {Canada}
	9. IP67 voor vochtbestendigheid
	10. IK10 voor slagvastheid
5. Desktoplezers moeten voldoen aan de volgende normen:
	1. EN 301 489-1 voor EMC {EU}
	2. EN 300 330 voor radio {EU}
	3. IEC/EN 60950-1 voor veiligheid {EU}
	4. FCC deel 15C voor radio {US}
	5. RSS-GEN, 210 voor radio {Canada}
	6. UL/CSA 62368-1 voor veiligheid {VS/Canada}

1.9   ALGEMENE EISEN VOOR FUNCTIONALITEIT

1. Door gebruik te maken van een proximity-lezer moet het mogelijk zijn de inloggegevens van een gebruiker te lezen.
	1. Een gebruiker van een credential moet zijn tag of smart-credential aan de lezer kunnen presenteren om geldige toegang tot een toegangspunt te krijgen.
		1. Het aanbieden van een ongeldig credential geeft geen toegang.
	2. Een gebruiker van een credential moet zijn tag aan de lezer kunnen aanbieden om een apparaat te bedienen.
		1. Het presenteren van een ongeldige identificatie heeft geen invloed op het apparaat.
	3. Er wordt visuele feedback aan de gebruiker gegeven op vertoon van een credential.
		1. Feedback zal aangeven of de credential geldig of ongeldig is voor de beoogde actie.
	4. Er wordt hoorbare feedback aan de gebruiker gegeven op vertoon van een identificatie.
		1. Feedback zal aangeven of de identificatie geldig of ongeldig is voor de beoogde actie.
2. Door gebruik te maken van een keyboardlezer moet het voor een gebruiker mogelijk zijn een pincode of code in te voeren om zichzelf te identificeren.
	1. Het is mogelijk om een pincode of code te gebruiken in combinatie met een proximity tag of smartcredential om de veiligheid te verhogen.
	2. Het systeem vereist een gebruikersauthenticatiemodus die geschikt is voor het apparaat of toegangspunt waarmee interactie plaatsvindt. De bedrijfsmodus zal zichzelf automatisch veranderen op verschillende tijdstippen van de dag of dagen van de week, afhankelijk van de configuratie.
3. Alle lezers die aan de buitenrand van de locatie worden gebruikt, moeten vanwege de veiligheid een IK10-classificatie hebben.
4. Het moet mogelijk zijn om lezers te mixen en matchen om aan de vereisten van het project te voldoen:
5. Lezers moeten op de deurcontroller worden aangesloten:
	1. Lezers communiceren met de deurcontroller
	2. Lezers worden gevoed door de deurcontroller.
6. Het systeem registreert toegangs- en apparaatgebeurtenissen.
	1. Er wordt een gebeurtenis gegenereerd voor de volgende activiteit:
		1. Nadat een geldige credential is gelezen, wanneer de deur wordt ontgrendeld.
		2. Nadat een ongeldige credential is gelezen en de deur niet is ontgrendeld.
		3. Wanneer de deur wordt geforceerd.
		4. Wanneer de deur openblijft, deur te lang open.
		5. Wanneer meerdere onjuiste cijfers worden ingevoerd op een keypadlezer, wat resulteert in een sabotage.
	2. Er wordt een gebeurtenis gegenereerd bij inbraak integratie:
		1. Nadat een geldige credential is gelezen, wordt het alarm ingeschakeld.
		2. Nadat een geldige credential is gelezen, wordt het alarm uitgeschakeld.
		3. Nadat een ongeldige credential is gelezen.
	3. Er wordt een gebeurtenis gegenereerd voor de volgende apparaatactiviteit:
		1. Nadat een geldige credential is gelezen en een apparaat wordt in- of uitgeschakeld.
		2. Nadat een ongeldige credential is gelezen.
	4. Alle gebeurtenissen worden voorzien van een tijd- en datumstempel.
	5. Bij alle gebeurtenissen moet worden vermeld op welke deur of welk apparaat ze betrekking hebben.
	6. Alle gebeurtenissen worden in realtime met de server gecommuniceerd
7. Het systeem moet gebruiksvriendelijk zijn:
	1. Het systeem blijft operationeel terwijl de server offline is.
	2. Elke deurcontroller en bijbehorende lezers blijven standalone operationeel zolang het netwerk of andere controllers niet beschikbaar zijn.
	3. Elke deurcontroller moet worden uitgerust met een back-up accu, zodat de deurcontroller en de kaartlezers kunnen blijven werken tijdens een stroomuitval. {Verwijderen als er geen accu is geplaatst}
		1. De accu wordt door het systeem bewaakt en geeft de huidige status en lading weer in de gebruikersinterface.

1.10 ALGEMENE EISEN VOOR COMMUNICATIE

1. Deurcontroller naar lezer
	1. 1.       Lezers communiceren met een deurcontroller via de volgende, of technisch gelijkwaardige, kabel:
		1. 22AWG, 4-aderig gedraaid paar
			1. De maximale kabellengte bedraagt 100 m (328')
	2. Alle lezers worden zonder extra kosten geleverd met 5 m (16,4') 22AWG 4-aderige twisted pair-kabel.
	3. Alle lezers communiceren via een RS485-protocol.
	4. Elke deurcontroller ondersteunt minimaal 2 beraadde lezers.
	5. Lezers worden automatisch gedetecteerd door de deurcontroller.
	6. Er is geen handmatige adressering vereist.
2. Computer-naar-desktoplezer
	1. Desktoplezers communiceren met een client-pc via de volgende kabel:
		1. Mini-USB naar USB
	2. De desktoplezer voert kaart nummer gegevens in de Paxton10-software in via een client-pc.
	3. De desktoplezer moet plug-and-play zijn en gebruik maken van een keyboard output.
3. Het systeem maakt gebruik van standaard netwerkprotocollen om installatie op de bedrijfsinfrastructuur mogelijk te maken.

DEEL 2         PRODUCTEN

2.1     FABRIKANTEN

1. Voorgeschreven fabrikant: Paxton
	1. E-mailadres:
		1. {NL} [support@paxton-benelux.com]
	2. Telefoonnummer:
		1. {NL} [076 3333 999]
	3. Website
		1. www.paxton-benelux.com
2. Alternatieven producten niet toegestaan. {Verwijder indien nodig}
3. De componenten van het systeem moeten van één enkele fabrikant zijn om de compatibiliteit van het systeem te garanderen.
4. De fabrikant van de lezer moet ook het hele toegangscontrolesysteem leveren.
5. De fabrikant van de lezer moet ook het deurintercom systeem leveren.
6. Beperkingen tijdens vervangen
	1. Het moet mogelijk zijn om de kaartlezer aan een bestaand [Paxton10] systeem toe te voegen.
	2. Het moet mogelijk zijn een lezer te installeren als functionele vervanging van een bestaande lezer.

2.2 SPECIFIEKE EISEN VOOR kaarten en tags

{Verwijderen wanneer niet nodig}

1. De fabrikant van de lezer kan Paxton HiTag2 125KHz-tokens leveren.
	1. De geleverde tokens zullen een authenticatiemethode bevatten om het kopiëren en ongeoorloofd gebruik van tokens te voorkomen.

2.3 SPECIFIEKE EISEN VOOR [PAXTON10] READERS
{Verwijderen wanneer niet nodig}

1. Kenmerken
	1. De kaartlezer bevat multiformat leestechnologie, die ondersteuning biedt voor meerdere kaartformaten van credentials tegelijk.
	2. De kaartlezer moet Bluetooth Low Energy (BLE)-ondersteuning bevatten om communicatie met mobiele en draagbare apparaten mogelijk te maken.
	3. De kaartlezer moet snel en eenvoudig kunnen worden geïnstalleerd.
	4. De kaartlezer is energiezuinig en maakt gebruik van een energiezuinige slaapmodus met capacitieve wake-up sensor.
	5. De kaartlezer heeft een IP-classificatie voor extern gebruik.
2. Identificatie van credential
	1. De kaartlezer bevat een proximity-lezer.
		1. Minimaal wordt de volgende kaart lees technologie ondersteund:
			1. Paxton Hitag2 125 kHz
			2. EM4100/02
			3. EM4200
			4. Sony FeliCa Lite-S
			5. MIFARE 1K
			6. MIFARE 4K
			7. MIFARE Ultralight / C
			8. MIFARE DESFire / EV1
			9. MIFARE Mini
			10. HID 125 kHz
			11. Bluetooth Smartcredential
		2. Alle bovengenoemde kaarttechnologie wordt gelijktijdig ondersteund.
		3. De volgende kaartformaten van credentials worden ondersteund:
			1. ISO-kaart
			2. Clamshell
			3. Minifob/sleutelhanger
			4. Proxidisc
			5. Watchprox
			6. Handsfree token
			7. Smartphone
			8. Bluetooth Smart-apparaat
			9. Smartwatch Bluetooth-apparaat
		4. Het kaartleesbereik, bij binnentemperatuur, moet voor elk credentialtype minimaal zijn:
			1. Hitag2

ISO-kaart – 2,2" (57 mm)

Clamshell – 2,2" (57 mm)

Minifob – 1,1" (29 mm)

Proxdisc – 1,7" (43 mm)

Horlogeprox – 0,5" (12 mm)

* + - 1. EM

EM-minifob – 1" (26 mm)

EM Proxdisc – 1,3" (32 mm)

EM4100 ISO-kaart – 1,7" (43 mm)

EM4200 ISO-kaart – 1,2" (30 mm)

* + - 1. MIFARE

Magnadata 1443 1k – 1,5" (39 mm)

Magnadata 1443 4k – 1,6" (40 mm)

NXP Klassiek 1K – 1,8" (45 mm)

NXP Klassiek 4K – 1,5" (38 mm)

Magnadata DESFire – 1,1" (29 mm)

NXP PLUS S – 1,2" (30 mm)

NXP Ultralicht – 1,7" (44 mm)

R5 – 1" (26 mm)

Felica – 1,4" (36 mm)

* + - 1. HID

36-bits – 1,3" (34 mm)

34-bits – 1,1" (29 mm)

26-bits – 1,3" (32 mm)

* + 1. Het Bluetooth-leesbereik moet configureerbaar zijn in de toegangscontrole software.
			1. De volgende Bluetooth-modus zijn beschikbaar:

Bluetooth uitgeschakeld

Korte afstand/aanbied-modus

Touch to enter, zonder credential aanbieden

Lange afstand/ hands free

1. Voeding
	1. De kaartlezer werkt op gelijkstroom die wordt geleverd door de deurcontroller.
		1. Er is geen extra stroombron nodig.
	2. De bedrijfsspanning mag niet hoger zijn dan 12 V DC.
	3. Het stroomverbruik tijdens inactiviteit mag niet hoger zijn dan 0,5 W.
		1. Het moet mogelijk zijn Bluetooth-communicatie uit te schakelen, waardoor het energieverbruik verder kan worden verminderd.
2. Communicatie
	1. Het moet mogelijk zijn om de lezer op een afstand van minimaal 100 meter van de controller te plaatsen zonder dat de communicatie wordt belemmerd.
	2. De kaartlezer zal zich aanmelden bij de controller om automatische detectie mogelijk te maken.
		1. De kaartlezer moet het serienummer en het type lezer communiceren met de deurcontroller.
	3. De kaartlezer communiceert zijn functionele status wanneer de deurcontroller daarom vraagt.
	4. De kaartlezer communiceert kaartgegevens van verschillende formaten en lengtes.
	5. De kaartlezer communiceert met credentials via:
		1. 125 kHz radiofrequentie
		2. 13,56 MHz radiofrequentie
		3. 2,4 GHz radiofrequentie
3. Weergave
	1. De kaartlezer bevat een stijlvole LED-aanduiding.
		1. Deze zal bestaan uit één enkele RGB LED.
	2. De LED geeft de volgende status en gebeurtenissen aan:
		1. Geldige credential gelezen
		2. Ongeldige credential gelezen
			1. Ongeldige toegang
			2. Onbekende credential
			3. Geblokkeerde credential
		3. Inbraakalarm inschakelen
		4. Inbraakalarm ingeschakeld
		5. Inbraakalarm uitgeschakeld
		6. Deur ontgrendeld
		7. Uitgang ingeschakeld
	3. De status LED blijft aan wanneer de lezer in rust is zodat deze beter gevonden kan worden in onverlichte omgevingen.
		1. Het moet mogelijk zijn de status LED uit te schakelen wanneer de lezer in rust is.
4. Audio
	1. De kaartlezer moet een piëzozoemer bevatten voor hoorbare feedback
	2. Er klinkt een pieptoon om de volgende gebeurtenissen aan te geven:
		1. Geldige credential gelezen – toegang verleend
		2. Ongeldige credential gelezen – toegang geweigerd
			1. Ongeldige autorisatie
			2. Onbekende credential
			3. Geblokkeerde credential
	3. Het moet mogelijk zijn de piëzozoemer uit te schakelen om een stille werking te garanderen.
5. Temperatuur
	1. De kaartlezer moet voldoen aan de vereiste temperatuurnormen voor een extern product
		1. De kaartlezer zal betrouwbaar functioneren binnen het temperatuurbereik van -35°C tot +66°C.
6. Behuizing
	1. De kaartlezer moet stijlvol en modern zijn.
	2. De kaartlezer heeft een laag profiel.
	3. Er mogen geen zichtbare bevestigingen op de kaartlezer aanwezig zijn.
	4. Het materiaal van de behuizing moet bestaan uit PC en ABS
	5. De kaartlezer is verkrijgbaar in het zwart
	6. De volgende montageopties zijn beschikbaar:
		1. Bevestiging aan een oppervlak
7. Afmetingen
	1. De afmetingen mogen niet groter zijn dan:
		1. Een breedte van 49 mm
		2. Een hoogte van 104 mm
		3. Een diepte van 17,2 mm

2.4 SPECIFIEKE EISEN VOOR [PAXTON10] LEZER KEYPADS
{Verwijderen wanneer niet nodig}

1. Kenmerken
	1. De kaartlezer bevat Multi format leestechnologie, die ondersteuning biedt voor meerdere kaartformaten van credentials tegelijk.
	2. De kaartlezer moet Bluetooth Low Energy (BLE)-ondersteuning bevatten om communicatie met mobiele en draagbare apparaten mogelijk te maken.
	3. De kaartlezer bevat een toetsenbord met 12 toetsen, dat ondersteuning biedt voor pincode- en code credentials.
	4. De kaartlezer biedt ondersteuning voor twee factorauthenticatie.
		1. De volgende werkingsmodus zijn beschikbaar:
			1. Alleen kaart
			2. Alleen pincode
			3. Alleen code
			4. Kaart + pincode
			5. Kaart + code
			6. Kaart of pincode
			7. Kaart of code
			8. Kaart, pincode of code
		2. Het moet mogelijk zijn om een specifieke werkingsmodus te selecteren tijdens gespecificeerde tijdschema's.
	5. Het systeem genereert een sabotage alarm na twintig toetsaanslagen zonder geldige pincode of code.
	6. De kaartlezer moet snel en eenvoudig kunnen worden geïnstalleerd.
	7. De kaartlezer moet energiezuinig zijn en gebruik maken van een energiezuinige slaapmodus met capacitieve wake up sensor.
	8. De kaartlezer heeft een IP-classificatie voor extern gebruik.
	9. De kaartlezer moet een IK-classificatie hebben wat betreft vandaalbestendigheid.
2. Identificatie van credential
	1. De kaartlezer bevat een proximity-lezer.
		1. Minimaal wordt de volgende kaart lees technologie ondersteund:
			1. Paxton Hitag2 125 kHz
			2. EM4100/02
			3. EM4200
			4. Sony FeliCa Lite-S
			5. MIFARE 1K
			6. MIFARE 4K
			7. MIFARE Ultralight / C
			8. MIFARE DESFire / EV1
			9. MIFARE Mini
			10. HID 125 kHz
			11. Bluetooth Smartcredential
		2. Alle bovengenoemde kaarttechnologie wordt gelijktijdig ondersteund.
		3. De volgende kaartformaten van credentials worden ondersteund:
			1. ISO-kaart
			2. Clamshell
			3. Minifob/sleutelhanger
			4. Proxidisc
			5. Watchprox
			6. Handsfree token
			7. Smartphone
			8. Bluetooth Smart-apparaat
			9. Smartwatch Bluetooth-apparaat
		4. Het kaartleesbereik, bij binnentemperatuur, moet voor elk credential type minimaal zijn:
			1. Hitag2

ISO-kaart – 52 mm

Clamshell – 55 mm

Minifob – 24 mm

Proxdisc – 37 mm

Horlogeprox – 10 mm

* + - 1. EM

EM-minifob – 24 mm

EM Proxdisc – 30 mm

EM4100 ISO-kaart – 38 mm

EM4200 ISO-kaart – 26 mm

* + - 1. MIFARE

Magnadata 1443 1k – 40 mm

Magnadata 1443 4k – 42 mm

NXP Klassiek 1K – 43 mm

NXP Klassiek 4K – 37 mm

Magnadata DESFire – 29 mm

NXP PLUS S – 28 mm

NXP Ultralicht – 46 mm

R5 – 24 mm

Felica – 36 mm

* + - 1. HID

36-bits – 28 mm

34-bits – 24 mm

26-bits – 29 mm

* + 1. Het Bluetooth-leesbereik moet configureerbaar zijn in de toegangscontrole software.
			1. De volgende Bluetooth-modus zijn beschikbaar:

Bluetooth uitgeschakeld

Korte afstand/aanbied-modus

Touch to enter, zonder credential aanbieden

Lange afstand / hands free

* 1. De lezer moet een keyboard bevatten.
		1. De volgende formaten van credentials worden ondersteund:
			1. Pincode
			2. Code
		2. Aan elke gebruiker kan een pincode worden toegewezen
			1. De lengte van de pincode kan worden geconfigureerd om aan de beveiligingsvereisten van het project te voldoen.
			2. Alle pincodes op het systeem moeten dezelfde lengte hebben.
			3. Het systeem ondersteunt een pincode van 4 tot 8 cijfers.
			4. Er zijn minimaal 100.000.000 mogelijke pincodecombinaties mogelijk.
			5. Een gebruiker kan zijn eigen pincode definiëren.
			6. Pincodes worden gebruikt om te identificeren welke gebruiker toegang heeft gekregen.
		3. Aan elk keypad kan een code worden toegewezen
			1. Het systeem ondersteunt codes met een lengte tussen 4 en 8 cijfers.
			2. Het systeem ondersteunt codes van verschillende lengtes.
			3. Aan elk apparaat kunnen meerdere codes worden toegewezen.
			4. Dezelfde code kan op meerdere apparaten worden gebruikt.
			5. Er zijn minimaal 111.110.000 mogelijke codecombinaties.
			6. Codes zijn algemeen en identificeren de gebruiker niet. De gebruiker wordt alleen geïdentificeerd als hij een kaart + code gebruikt.
1. Voeding
	1. Het kaartlezer werkt op gelijkstroom die wordt geleverd door de controller.
		1. Er is geen extra stroombron nodig.
	2. De bedrijfsspanning mag niet hoger zijn dan 12 V DC.
	3. Het stroomverbruik tijdens inactiviteit mag niet hoger zijn dan 0,5 W.
		1. Het moet mogelijk zijn Bluetooth-communicatie uit te schakelen, waardoor het energieverbruik verder kan worden verminderd.
2. Communicatie
	1. Het moet mogelijk zijn om de lezer op een afstand van minimaal 100 meter van de controller te plaatsen zonder dat de communicatie wordt belemmerd.
	2. Het kaartlezer zal zijn aanwezigheid melden aan de controller om automatische detectie mogelijk te maken.
		1. Het kaartlezer moet het serienummer en het type lezer communiceren.
	3. Het kaartlezer communiceert zijn functionele status wanneer de verwerkingsverantwoordelijke daarom vraagt.
	4. Het kaartlezer communiceert tokengegevens van verschillende formaten en lengtes.
	5. Het kaartlezer communiceert met tokens via:
		1. 125 kHz radiofrequentie
		2. 13,56 MHz radiofrequentie
		3. 2,4 GHz radiofrequentie
3. Weergave
	1. Het artikel bevat een stijlvol LED-display.
		1. Deze zal bestaan ​​uit één enkele RGB LED.
	2. De LED geeft de volgende toestanden en gebeurtenissen aan:
		1. Geldige referentie gelezen
			1. Geldig token
			2. Geldige pincode
			3. Geldige code
		2. Ongeldige inloggegevens gelezen
			1. Ongeldige machtigingen
			2. Onbekende identificatie
			3. Geblokkeerde identificatie
			4. Alarm voor sleutelhacker
		3. Twee factorauthenticatie
			1. Vereist een pincode om het verzoek te voltooien
			2. Vereist code om het verzoek te voltooien
		4. Inbraakalarm inschakelen
		5. Inbraakalarm ingeschakeld
		6. Inbraakalarm uitgeschakeld
		7. Deur ontgrendeld
		8. Uitgang ingeschakeld
	3. De LED blijft standaard aan om ondersteuning te bieden bij het lokaliseren van de lezer in onverlichte omgevingen.
		1. Het moet mogelijk zijn de LED tijdens inactiviteit uit te schakelen.
4. Audio
	1. Het item moet een piëzozoemer bevatten voor hoorbare feedback
	2. Er klinkt een toon om aan te geven dat er op een toets wordt gedrukt.
	3. Er klinkt een toon om de volgende gebeurtenissen aan te geven:
		1. Geldige inloggegevens gelezen – toegang verleend
		2. Icoon voor Geverifieerd door de community
		3. Icoon voor Geverifieerd door de community
			1. Onbekende identificatie
			2. Geblokkeerde identificatie
	4. Het moet mogelijk zijn de hoorbare feedback uit te schakelen om een ​​stille werking te garanderen.
5. Temperatuur
	1. Het artikel moet voldoen aan de vereiste temperatuurnormen voor een extern product
		1. Het item zal betrouwbaar functioneren binnen het temperatuurbereik van 0°C tot 65°C

(-35°C to +66°C).

1. Behuizing
	1. De kaartlezer moet stijlvol en modern zijn.
	2. De kaartlezer heeft een laag profiel.
	3. Er mogen geen zichtbare bevestigingen op het artikel aanwezig zijn.
	4. Het materiaal van de behuizing moet bestaan ​​uit PC en ABS
	5. Het toetsenbordmateriaal moet van gehard siliconen zijn
	6. Het artikel is verkrijgbaar in het zwart
	7. De volgende montageopties zijn beschikbaar:

a. Bevestiging aan een oppervlak

b. US Backbox-montage (via een backbox-adapter)

1. Afmetingen
	1. De afmetingen mogen niet groter zijn dan:
		1. Een breedte van 2,5 "(63,8 mm)
		2. Een hoogte van 4,1 "(104 mm)
		3. Een diepte van 18,2 mm (0,7 inch)

2.5                SPECIFIEKE EISEN VOOR [PAXTON10] VANDAALBESTENDIGE LEZER

1. Kenmerken
	1. Het item bevat leestechnologie voor meerdere formaten, die ondersteuning biedt voor meerdere formaten van legitimatiebewijzen tegelijk.
	2. Icoon voor Geverifieerd door de community
	3. Het artikel moet snel en eenvoudig kunnen worden geïnstalleerd.
	4. Het artikel is energiezuinig en maakt gebruik van een energiezuinige slaapmodus met capacitief ontwaken.
	5. Het artikel heeft een IP-classificatie voor extern gebruik.
	6. Het artikel moet een IK-classificatie hebben wat betreft vandaalbestendigheid.
2. Identificatie van identificatiegegevens

1.  Het artikel bevat een proximity-lezer.

* + 1. Minimaal wordt de volgende tokentechnologie ondersteund:
			1. Paxton Hitag2 125kHz
			2. EM4100/02
			3. EM4200
			4. Sony FeliCa Lite-S
			5. MIFARE 1K
			6. MIFARE 4K
			7. MIFARE Ultralight / C
			8. MIFARE DESFire / EV1
			9. MIFARE Mini
			10. HID 125kHz
			11. Bluetooth Smart
		2. Alle bovengenoemde tokentechnologie wordt gelijktijdig ondersteund.
		3. De volgende formaten van legitimatiegegevens worden ondersteund:
			1. ISO card
			2. Clamshell
			3. Minifob / sleutelhanger
			4. Proxidisc
			5. Watchprox
			6. Handsfree token
			7. Smartphone
			8. Bluetooth Smart-apparaat
		4. Het token leesbereik, bij binnentemperatuur, moet voor elk tokentype minimaal zijn:
			1. Icoon voor Geverifieerd door de community
				1. ISO card – 2.4" (61mm)
				2. Clamshell – 2.3" (58mm)
				3. Minifob – 0.9" (24mm)
				4. Proxdisc – 1.6" (40mm)
				5. Watchprox – 0.7" (19mm)
			2. EM
				1. EM-minifob – 1" (26 mm)
				2. EM Proxdisc – 1,3" (32 mm)
				3. EM4100 ISO-kaart – 1,8" (46 mm)
				4. EM4200 ISO-kaart – 1,4" (36 mm)
			3. MIFARE
1. Magnadata 1443 1k – 1,1" (28 mm)
2. Magnadata 1443 4k – 0,3" (8 mm)
3. NXP Klassiek 1K – 0,7" (18 mm)
4. NXP Klassiek 4K – 1,1" (28 mm)
5. Magnadata DESFire – 1,1" (28 mm)
6. NXP PLUS S – 1,1" (28 mm)
7. NXP Ultralicht – 1,1" (28 mm)
8. R5 – 0.9" (24mm)
9. Felica – 1.1" (28mm)
	* + 1. HID
10. 36 bit – 1.2" (30mm)
11. 34 bit – 0.9" (22mm)
12. 26 bit – 1.3" (32mm)
	* 1. Het Bluetooth-leesbereik moet configureerbaar zijn in de systeemsoftware.
			1. De volgende Bluetooth-modi zijn beschikbaar:

0Bluetooth uitgeschakeld

* + - * 1. Korte afstand/token-modus
				2. Aanraken om / zakbereik te openen
				3. Lange afstand
1. Voeding
	1. Het item werkt op gelijkstroom die wordt geleverd door de controller.
		1. Er is geen extra stroombron nodig.
	2. De bedrijfsspanning mag niet hoger zijn dan 12 V DC.
	3. Het stroomverbruik tijdens inactiviteit mag niet hoger zijn dan 0,5 W.
		1. Icoon voor Geverifieerd door de community
2. Communicatie
	1. Het moet mogelijk zijn om de lezer op een afstand van minimaal 100 meter van de controller te plaatsen zonder dat de communicatie wordt belemmerd.
	2. Het kaartlezer zal zijn aanwezigheid melden aan de controller om automatische detectie mogelijk te maken.
		1. Het kaartlezer moet het serienummer en het type lezer communiceren.
	3. Het kaartlezer communiceert zijn functionele status wanneer de verwerkingsverantwoordelijke daarom vraagt.
	4. Het kaartlezer communiceert tokengegevens van verschillende formaten en lengtes.
	5. Het kaartlezer communiceert met tokens via:
		1. 125 kHz radiofrequentie
		2. 13,56 MHz radiofrequentie
		3. 2,4 GHz radiofrequentie
3. Weergave
	1. Het artikel bevat een stijlvol LED-display.
		1. Deze zal bestaan ​​uit één enkele RGB LED.
	2. De LED geeft de volgende toestanden en gebeurtenissen aan:
		1. Geldige referentie gelezen
		2. Ongeldige inloggegevens gelezen
			1. Ongeldige machtigingen
			2. Onbekende identificatie
			3. Geblokkeerde identificatie
		3. Inbraakalarm inschakelen
		4. Inbraakalarm ingeschakeld
		5. Inbraakalarm uitgeschakeld
		6. Deur ontgrendeld
		7. Uitgang ingeschakeld
	3. De LED blijft standaard aan om ondersteuning te bieden bij het lokaliseren van de lezer in onverlichte omgevingen.
		1. Icoon voor Geverifieerd door de community
4. Audio
	1. Het item moet een piëzozoemer bevatten voor hoorbare feedback
	2. Er klinkt een toon om de volgende gebeurtenissen aan te geven:
		1. Geldige inloggegevens gelezen – toegang verleend
		2. Ongeldige inloggegevens gelezen – toegang geweigerd
			1. Icoon voor geverifieerd door de community
			2. Onbekende identificatie
			3. Geblokkeerde identificatie
	3. Het moet mogelijk zijn de hoorbare feedback uit te schakelen om een ​​stille werking te garanderen.
5. Temperatuur
	1. Het artikel moet voldoen aan de vereiste temperatuurnormen voor een extern product
		1. Het item zal betrouwbaar functioneren binnen het temperatuurbereik van -31°F tot +150,8°F

(-35°C tot +66°C).

1. Huisvesting
	1. De kaartlezer heeft een laag profiel.
	2. Het materiaal van de behuizing moet bestaan ​​uit PC, ABS en ASTM B86
	3. De volgende montageopties zijn beschikbaar:

a. Bevestiging aan een oppervlak

1. Afmetingen
	1. De afmetingen mogen niet groter zijn dan:
		1. Een breedte van 2,3 inch (57,6 mm)
		2. Een hoogte van 4,2 "(106 mm)
		3. Een diepte van 19,5 mm (0,8")

2.6  SPECIFIEKE EISEN VOOR DESKTOPLEZER

1. Kenmerken
	1. De desktoplezer moet het toewijzen van tokens aan gebruikers vergemakkelijken.
	2. De desktoplezer moet meerdere typen en formaten proximity-tokens lezen.
	3. De desktoplezer identificeert tokens/inloggegevens die al aan gebruikers zijn toegewezen.
	4. De desktoplezer is het niet meer noodzaak om het nummer van elk token te kennen.
	5. In systemen met meerdere client-pc's moet het systeem meerdere desktoplezers kunnen ondersteunen.
	6. De desktoplezer zal een unieke ID van elk gepresenteerd token weergeven.
	7. De desktoplezer zal een unieke ID uit verschillende formaten en lengtes weergeven.
2. Gebruikersinteractie
	1. De desktoplezer werkt in een intuïtieve modus:
		1. Wanneer een niet-toegewezen token/referentie wordt gepresenteerd, zal de systeemsoftware automatisch het gebruikersrecord en het gebruikersscherm creëren voor het invoeren van gebruikersinformatie en andere beveiligingsinstellingen.
		2. Wanneer de software beheerder zich al in een gebruikersrecord bevindt en een niet-toegewezen token/credential wordt gepresenteerd, zal de software de optie weergeven om het token/credential aan het huidige record toe te voegen.
		3. Wanneer een bestaande token/credential aan de desktoplezer wordt gepresenteerd, haalt de software automatisch de gebruikersrecord op die aan die gebruiker is gekoppeld en geeft deze weer. Als er meerdere tokens/referenties aan die gebruiker zijn toegewezen, zal de software de specifieke weergegeven tokens markeren.
	2. De lezer moet plug & play zijn.
3. Proximity-lezer
	1. Het artikel bevat een proximity-lezer.
		1. Minimaal wordt de volgende tokentechnologie ondersteund:
			1. Paxton HiTag2 125KHz
			2. HID 125KHz
			3. EM4100/02
			4. EM4200
			5. Sony FeliCa Lite-S
			6. MIFARE 1K
			7. MIFARE 4K
			8. MIFARE Ultralight / C
			9. MIFARE DESFire / EV1
			10. MIFARE Mini
		2. Alle bovengenoemde tokentechnologie wordt gelijktijdig ondersteund.
		3. De volgende formaten van legitimatiegegevens worden ondersteund:
			1. ISO-kaart
			2. Clamshell
			3. Minifob/sleutelhanger
			4. Proxidisc
			5. Watchprox
			6. Handsfree token
4. Voeding
	1. Het item wordt gevoed via USB.
5. Communicatie
	1. De desktoplezer wordt aangesloten op een pc via een mini-USB-naar-USB-kabel.
6. Display
	1. Het artikel bevat een stijlvol LED-display.

2.  De LED's geven de volgende toestanden aan:

a. Artikel aangedreven / klaar voor gebruik

1. Temperatuur

1.    Het artikel moet voldoen aan de vereiste temperatuurnormen voor een inwendig product

a. Het item werkt betrouwbaar binnen het temperatuurbereik van 0 °C tot +49 °C (32 °F tot 120 °F) Huisvesting

* 1. Het artikel moet stijlvol en modern zijn.
	2. Het product is verkrijgbaar in het zwart
1. Afmetingen
2. De afmetingen van de desktoplezer mogen niet groter zijn dan:
	* 1. A width of 115mm (4.5")
		2. Een hoogte van 19 mm (0,7")
		3. Een diepte van 75 mm (3")

END OF SECTION