

Algemene informatie

Aanbesteding: Digitale sluitsystemen
Aanbestedende Dienst: Hoogheemraadschap van Schieland en de Krimpenerwaard
Referentie: A0231

Toelichting:

Hierbij de eerste Nota van Inlichtingen. Wedervragen kunnen worden gesteld tot en met 11 november 2024, 10:00 uur.

Vraag en antwoord

Ref.nr.	Onderwerp:
1	Bijlage 5

Vraag:

In de tekst in de bijlage 5 staan de volgende regels:

- Minimaal twee installaties op een terrein aan de toegangspoort;
- Minimaal vijf afzonderlijk gesitueerde gebouwen en/of locaties.

Wordt hiermee aangegeven dat inschrijver ook in staat moet zijn om toegangspoorten aan te sturen binnen het geheel van de opdracht? Graag aangeven of dit de juiste aanname betreft.

Antwoord:

Deze aanname klopt niet, aanbestedende dienst bedoelt hiermee het aantoonbaar leveren en installeren van twee digitale cilindersloten op de toegangspoort van het terrein en het leveren en installeren van vijf digitale cilindersloten in afzonderlijk gesitueerde gebouwen en/of locaties.

Percelen: P1 Digitale Sluitsystemen
Beantwoord op: 30 okt. 2024

Ref.nr.	Onderwerp:
2	Bijlage 6

Vraag:

Kan de aanbestedende dienst aangeven hoe vaak, absoluut en relatief, het voorgekomen is in de afgelopen 2 jaar dat als gevolg van de 24/7 bereikbaarheid er een inzet buiten de reguliere werktijden is geweest?

Antwoord:

Dit kan aanbestedende dienst niet aangeven. Dit is de eerste keer dat een dergelijke digitaal sluitsysteem wordt geïntroduceerd en aangelegd. Derhalve zijn er geen historische gegevens van digitale sluitsystemen bekend bij de

aanbestedende dienst.

Percelen: P1 Digitale Sluitsystemen
Beantwoord op: 30 okt. 2024

Ref.nr.
3

Onderwerp:
Bijlage 2 - Programma van Eisen, Blz. 6. Hoofdstuk Technische- en functionele eisen, hangsloten

Vraag:
Veiligheidsklasse 4 en 5: De behuizing moet zo zijn ontworpen dat de leesunit zodanig is beveiligd dat de functie gegarandeerd is, ook bij uitval
Wat wordt er bedoeld 'ook bij uitval'? Naar welke veiligheidsklasse wordt gerefereerd met klasse 4 / 5? Kan dit nader gespecificeerd worden?

Antwoord:
Met uitval wordt bedoeld het niet functioneren van het digitale component voor het openen en sluiten van het cilinderslot.

Hangsloten worden ingedeeld in SKG sterrenclassificatie, die verwijzen naar de mate van bescherming die ze bieden. Deze klassen worden vastgesteld op basis van de testen die in de EN 12320-norm zijn beschreven prestatie-eisen 1 t/m 6.

In de norm worden hangsloten gecategoriseerd op basis van hun weerstand tegen verschillende soorten aanvallen en slijtage. Hoewel de norm zelf niet expliciet spreekt over "veiligheidsklassen" zoals klasse 4 of 5, definieert het wel prestatie-eisen waaraan een hangslot moet voldoen.

Veiligheidsklasse 4 wordt geassocieerd met sloten die uitblinken in meerdere prestatiecategorieën in de EN 12320-tests, meestal met scores van 5 of 6 in belangrijke categorieën zoals weerstand tegen zagen, trekken en boren. Deze sloten bieden zeer sterke beveiliging tegen agressieve aanvallen, zoals met zware gereedschappen.

Veiligheidsklasse 5 verwijst naar de maximale beveiliging. Sloten in deze klasse moeten in bijna elke categorie uit de EN 12320-norm hoge scores behalen (meestal 6 in de meeste categorieën). Ze zijn ontworpen om weerstand te bieden tegen de meest krachtige aanvallen, inclusief thermische aanvallen (zoals branders) en professionele inbraakpogingen.

De EN 12320-norm bevat testmethodes en prestatiecriteria voor de volgende zes eigenschappen van hangsloten:

1. Corrosieweerstand
2. Weerstand tegen torsie (draaikracht)
3. Weerstand tegen zagen
4. Weerstand tegen trekken
5. Weerstand tegen knippen

6. Weerstand tegen manipulatie

Voor elke eigenschap wordt een score gegeven op een schaal van 1 tot 6, waarbij 6 de hoogste en sterkste beveiliging vertegenwoordigt.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.

4

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 6. Hoofdstuk Technische- en functionele eisen, Fysieke digitale (oplaadbare) sleutel

Vraag:

De fysieke digitale sleutel maakt gebruik van NFC-technologie en voorziet hiermee de batterij loze digitale sluitcomponenten van de benodigde energie. Is een andere vorm van communicatie, waarmee BLE technologie vanuit de telefoon (IOS + Android) wordt ondersteund, toegestaan?

Antwoord:

Dit is niet toegestaan, het toepassen van andere interfaces, zoals Bluetooth Low Energy (BLE) voor het updaten van digitale sleutels kan vanuit een beveiligingsperspectief niet worden toegestaan. Enkele redenen hiervoor zijn:

Beveiligingsrisico's: NFC (Near Field Communication) vereist dat apparaten zeer dicht bij elkaar worden gehouden (meestal binnen enkele centimeters), waardoor het risico op ongewenste toegang of af luisteren minimaal is. BLE daarentegen heeft een veel groter bereik, wat het makkelijker maakt voor kwaadwillenden om signalen op te vangen en mogelijk te manipuleren.

Risico op ongeoorloofde toegang: Omdat BLE verbinding maakt over een grotere afstand, vergroot dit de kans dat ongeautoriseerde personen toegang proberen te krijgen tot de gegevens of updates. NFC is in dit opzicht veiliger, omdat het fysiek contact nabij vereist.

Stroomverbruik en batterijverbruik: BLE kan voor sommige apparaten intensiever zijn qua batterijverbruik bij regelmatig gebruik, wat een praktische beperking vormt voor de smartphone van de gebruiker. NFC verbruikt daarentegen zeer weinig stroom en is specifiek ontworpen voor korte, directe interacties zoals toegang tot digitale sloten.

Beperking tot betrouwbare interface: Het gebruik van één consistente interface (zoals NFC) minimaliseert de complexiteit en verhoogt de veiligheid, omdat beheerders niet verschillende protocollen hoeven te beheren en beveiligen.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.

5

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 6. Hoofdstuk Technische- en functionele eisen, Fysieke digitale(oplaadbare) sleutel

Vraag:

De sleutelhanger beschikt over een geïntegreerde NFC- en Bluetooth-interface (BLE - Bluetooth Low Energy).
Er wordt hier sleutelhanger benoemd. Mag dat in dit geval ook een andere vorm hebben waarmee een elektronische cilinder geopend kan worden?

Antwoord:

Ja, een smartphone die gebruik maakt van NFC technologie.

Percelen:

P1 Digitale Sluitsystemen

Beantwoord op:

30 okt. 2024

Ref.nr.

6

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 6. Hoofdstuk Technische- en functionele eisen, Fysieke digitale (oplaadbare) sleutel

Vraag:

Kopieerbeveiliging gewaarborgd doormiddel van data encryptie met AES 256 protocol.
Mag de data encryptie ook voorzien zijn met AES 128 protocol met aanvullende (fysieke) beveiliging (zoals bijvoorbeeld een hack attack detectie op de chip zelf)?

Antwoord:

Nee, opdrachtgever heeft vergelijkbaar getest. Dit bleek niet te voldoen aan de beveiligingsvereisten van aanbestedende dienst.

Percelen:

P1 Digitale Sluitsystemen

Beantwoord op:

30 okt. 2024

Ref.nr.

7

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7. Hoofdstuk Technische- en functionele eisen, Fysieke digitale (oplaadbare) sleutel

Vraag:

Externe identificatie van de vergrendelingsautorisatie moet niet mogelijk zijn. Wat wordt hiermee bedoeld? Kan dit nader gespecificeerd worden?

Antwoord:

Hier wordt door de opdrachtgever het volgende mee bedoeld dat de autorisatie om toegang te krijgen tot of gebruik te maken van het vergrendelingsmechanisme niet op een manier mag worden geïdentificeerd of benaderd zodat deze door onbevoegden kan worden misbruikt.

Beveiliging tegen externe aanvallen: De autorisatie voor het ontgrendelen of vergrendelen van deuren of andere toegangscontrolemechanismen moet zo zijn ingesteld dat deze niet gemakkelijk te achterhalen is door externe partijen. Dit betekent dat er geen zwakke plekken of identificatiemethoden moeten zijn die door kwaadwillende kunnen worden gebruikt om toegang te krijgen.

Minimaliseren van informatieoverdracht: Het systeem moet zo ontworpen zijn dat er geen duidelijke identificatie of transmissie van autorisatiegegevens plaatsvindt die door derden kunnen worden afgevangen. Dit kan onder andere inhouden dat er geen openbare toegang is tot systemen of protocollen die deze identificatie kunnen onthullen.

Beperken van toegangsmethoden: Het systeem zou moeten waarborgen dat de methoden voor toegang (zoals sleutels, codes, of biometrische gegevens) alleen door bevoegde gebruikers kunnen worden gegenereerd of gebruikt. Er mogen geen achterdeuren of onveilige methoden zijn die het voor onbevoegden mogelijk maken om toegang te krijgen.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.

8

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7. Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

De bewerking van sluitcomponenten, toegangsrechten en programmeertaken door Opdrachtgever moet gegarandeerd worden.

Wat wordt hiermee bedoeld? Kan dit nader gespecificeerd worden?

Antwoord:

De opdrachtgever behoudt zich het recht voor om ten alle tijden zelf het fysieke component aan te mogen passen, de toegangsrechten in beheer software voor wijzigen/toevoegen en verwijderen van zonder tussenkomst van derden. Bijvoorbeeld taken gerelateerd aan in regelen van cilindersloten en (fysieke) sleutels in breedste zin van woord.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.

9

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7 Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

Enkel de Opdrachtgever met beheerderautorisatie moeten met behulp van een wachtwoord en programmeertoken toegang hebben.
Wordt hier MFA mee bedoeld? Kan dit nader gespecificeerd worden?

Antwoord:

Er wordt door de opdrachtgever geen expliciete Multi-Factor Authenticatie (MFA) bedoeld, maar er worden wel twee authenticatiemiddelen gevraagd voor de toegang tot beheer omgeving.

Percelen:

P1 Digitale Sluitsystemen

Beantwoord op:

30 okt. 2024

Ref.nr.

10

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7 Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

Telkens wanneer de gebruiker de database opent, vraagt het systeem om beschikbare updates en importeert deze automatisch naar de computers van de Opdrachtgever.
I.v.m. security redenen kan dit ook onwenselijk zijn. Mag deze eis komen te vervallen?

Antwoord:

Dit is niet akkoord omdat frequente toetsing van toegekende toegangsrechten noodzakelijk is om onrechtmatige toegang te voorkomen. De security van het communicatieprotocol moet op een andere manier zijn gewaarborgd.

Percelen:

P1 Digitale Sluitsystemen

Beantwoord op:

30 okt. 2024

Ref.nr.

11

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7 Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

De lokale softwareclient moet draaien op Windows-besturingssystemen vanaf Windows XP.
Betekend dit de wens voor een on-premise oplossing of mag de oplossing

ook als SaaS oplossing worden aangeboden?

Antwoord:

Dit is niet akkoord omdat aanbestedende dienst on-premise oplossing wilt, zodat beveiligingsmaatregelen en updates door de organisatie zelf worden beheerd en afgestemd op het beveiligingsbeleid.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.
12

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7 Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

Er moeten minimaal 50 verschillende beheerzones ondersteund worden. Wat wordt bedoeld met een "beheerszone"? Kan dit nader gespecificeerd worden?

Antwoord:

Een beheerzone is een afgebakend groep met sluitsystemen waarbinnen een beheerder in één keer de toegang en autorisatie-instellingen kan regelen voor verschillende producten, zoals elektronische sluitsystemen. hangsloten etc.

Dit biedt organisaties de mogelijkheid om toegangsrechten, updates en beheerfuncties centraal te beheren voor een specifieke groep deuren of poorten binnen een groep (beheerzone).

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.
13

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 7 Hoofdstuk Software-eisen, Beheer (s)applicatie

Vraag:

De software biedt gedefinieerde uitvoeringsprotocollen van de gebruikersmedia, die door de sluitsysteembeheerder vrij kunnen worden geconfigureerd of gewijzigd
Wat wordt hiermee bedoeld? Kan dit nader gespecificeerd worden?

Antwoord:

Met "gedefinieerde uitvoeringsprotocollen van de gebruikersmedia" wordt bedoeld dat de software vooraf bepaalde regels en procedures hanteert voor de werking van toegangspassen of sleutels binnen het elektronische

sluitsysteem. Deze protocollen bepalen bijvoorbeeld hoe de gebruikersmedia communiceren met de sloten en hoe toegang wordt verleend.

De mogelijkheid voor de sluitsysteembeheerder om deze protocollen te configureren of aan te passen betekent dat de beheerder de vrijheid heeft om specifieke instellingen en regels in te stellen die passen bij de behoeften van de organisatie. Dit kan bijvoorbeeld inhouden:

Aanpassen van toegangsniveaus: De beheerder kan bepalen welke deuren, zones of afdelingen toegankelijk zijn voor specifieke gebruikersmedia.

Tijdelijke of tijdgebonden toegangsrechten: De protocollen kunnen zo worden ingesteld dat toegangspassen enkel op bepaalde tijden of dagen actief zijn.

Veiligheidsregels voor gebruikersmedia: Bijvoorbeeld dat toegangspassen automatisch verlopen na een bepaalde tijd of na een specifiek aantal pogingen tot toegang.

Mogelijkheid tot blokkeren of opnieuw toewijzen: Bij verlies of wijziging in de autorisatie van een gebruiker kan de beheerder snel een sleutel of pas blokkeren of opnieuw configureren zonder fysieke ingrepen.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.

14

Onderwerp:

Bijlage 2 - Programma van Eisen, Blz. 8 Hoofdstuk Software-eisen, Gebruikersapplicatie (app)

Vraag:

De NFC-interfaces voor smartphones bieden de mogelijkheid voor het ontgrendelen van digitale sluitsystemen

Mogen ook andere interfaces, zoals BLE voor het updaten via een Smartphone van een digitale sleutel, toegepast worden?

Antwoord:

Niet akkoord, het toepassen van andere interfaces, zoals Bluetooth Low Energy (BLE) voor het updaten van digitale sleutels kan vanuit een beveiligingsperspectief niet worden toegestaan. Enkele voorbeelden hiervoor zijn:

Beveiligingsrisico's: NFC (Near Field Communication) vereist dat apparaten zeer dicht bij elkaar worden gehouden (meestal binnen enkele centimeters), waardoor het risico op ongewenste toegang of afluisteren minimaal is. BLE daarentegen heeft een veel groter bereik, wat het makkelijker maakt voor kwaadwillenden om signalen op te vangen en mogelijk te manipuleren.

Risico op ongeoorloofde toegang: Omdat BLE verbinding maakt over een grotere afstand, vergroot dit de kans dat ongeautoriseerde personen toegang proberen te krijgen tot de gegevens of updates. NFC is in dit opzicht veiliger, omdat het fysiek contact nabij vereist.

Stroomverbruik en batterijverbruik: BLE kan voor sommige apparaten intensiever zijn qua batterijverbruik bij regelmatig gebruik, wat een praktische beperking vormt voor de smartphone van de gebruiker. NFC verbruikt daarentegen zeer weinig stroom en is specifiek ontworpen voor korte, directe interacties zoals toegang tot digitale sloten.

Beperking tot betrouwbare interface: Het gebruik van één consistente interface (zoals NFC) minimaliseert de complexiteit en verhoogt de veiligheid, omdat beheerders niet verschillende protocollen hoeven te beheren en beveiligen.

Percelen: P1 Digitale Sluitsystemen
Beantwoord op: 30 okt. 2024

Ref.nr.
15

Onderwerp:
Bijlage 2 - Programma van Eisen, Blz. 8 Hoofdstuk Software-eisen, Gebruikersapplicatie (app)

Vraag:
Om veiligheidsredenen zijn "beschermd" apparaten niet toegestaan. Is het mogelijk toe te lichten wat er bedoeld wordt met "beschermd" apparaten en waarom een beschermd apparaat juist een security risico zou zijn?

Antwoord:
Deze eis is per abuis in het programma van eisen geland en komt te vervallen.

Percelen: P1 Digitale Sluitsystemen
Beantwoord op: 30 okt. 2024

Ref.nr.
16

Onderwerp:
Bijlage 2 - Programma van Eisen, Blz. 9 Hoofdstuk: Referentie afbeeldingen

Vraag:
Er zijn door de opdrachtgever referentie afbeeldingen meegegeven van het digitale cilinderslot, het hangslot en de fysieke sleutel. De opdrachtgever wil een gelijkwaardig product dat aansluit bij de in het referentie materiaal aangegeven dimensionering en vormgeving.
Gelijkwaardigheid met betrekking tot dimensionering van cilinders,

hangsloten en fysieke sleutels is één. Maar is het ook toegestaan cilinders zonder lees knop aan de buitenzijde aan te bieden? Is het in plaats van de specifiek afgebeelde digitale sleutel, mogelijk hiervoor een sleutel met een andere dimensionering en vormgeving aan te bieden?

Antwoord:

Esthetisch gezien zou het voor opdrachtgever niet uit maken dat er geen leesknop aan de buitenzijde zit. Het meest belangrijke is dat in de cilindersloten zelf geen batterij aanwezig is in verband met het beheer en de onderhoudskosten.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024

Ref.nr.
17

Onderwerp:
Servicecontract

Vraag:

Is de gestelde beschikbaarheid "binnen"24 uur een fysieke beschikbaarheid op locatie of volstaat een digitale beschikbaarheid?

Antwoord:

Een digitale beschikbaarheid volstaat niet. Het betreft een fysieke beschikbaarheid op locatie.

Percelen: P1 Digitale Sluitsystemen

Beantwoord op: 30 okt. 2024