



Aansluitvoorwaarden Rijkspas RWS

Versie 1.4

Datum oktober 2016
Status Geldig vanaf publicatiedatum

Colofon

CD
Dir. Facilitair en Financiën

Griffioenlaan 2 Utrecht

Contactpersoon Ir. F. den Hartog
Projectmanager Rijkspas
M +31(0)6-51208645
frank.den.hartog@rws.nl

Auteur CD en CIV

Versiebeheer:

Versie	Datum	Auteur	Opmerking
0.4	29-11-2013	Frank den Hartog	Versie 2013
1.0	2-11-2015	Frank den Hartog	- Update lijst van TCS-en in RWS landschap - SAM module eisen toegevoegd
1.1	2-12-2015	Frank den Hartog	- Aanpassingen namen contactpersonen leveranciers
1.2	23-5-2016	Frank den Hartog	- Uitleg toegevoegd mbt CS - Verwijzing naar RIVA
1.3	13-9-2016	Frank den Hartog	- Verwijzingen naar kaders Rijk en RWS
1.4	24-10-2016	Frank den Hartog	- Aanpassingen nav review Lässlo van Engeland
			-

Colofon—2

Inleiding—5

1	Kaders Fysieke Beveiliging—7
1.1	Rijksbrede kaders—7
1.2	IenM RWS kaders—7
2	Rijkspas—9
2.1	Rijkspas binnen RWS—9
2.2	Rijkspas systeemlandschap RWS—9
3	Aansluitvoorwaarden Rijkspas—12
4	Standaard apparatuur RWS Rijkspas—14
4.1	Toegangscontrole systemen—14
4.2	Toegangscontrole componenten—14
4.3	Hang- en Sluitwerk—16
5	Standaard inrichtingen RWS panden met Rijkspas—17

Inleiding

Binnen de Rijksoverheid wordt sinds 2009 de Rijkspas gebruikt als multifunctionele smartcard.

Doelstelling van de Rijkspas is te komen tot een veilige, betrouwbare, gebruiksvriendelijke, efficiënt en effectief geregelde toegangscontrole bij de Rijksoverheid.

De Rijkspas is een multifunctionele smartcard (gebruikt door alle op Rijkspas aangesloten departementen en agentschappen, centraal geproduceerd door Morpho) die wordt gebruikt als:

- Identiteitsbewijs binnen het Rijk (interdepartementale afspraak)
- Toegangsmiddel voor fysieke toegang
- Toegangsmiddel tot systemen (logische toegang)

Om de Rijkspas te mogen gebruiken dient te worden voldaan aan:

- Normenkader Rijkspas (eis vanuit BZK)
- Toets techniek/verbindingen door NBV/Rijkspasbeheer
- Ketentest Rijkspas door IenM en RWS
- Toets beheermodel applicaties door RWS-CIV

In dit document wordt beschreven op welke wijze en onder welke voorwaarden panden van Rijkswaterstaat (RWS, agentschap onder het Ministerie van Infrastructuur en Milieu IenM) aangesloten moeten worden voor het gebruik van de Rijkspas als toegangsmiddel voor fysieke toegang.

Indien een toegangssysteem niet aan deze aansluitvoorwaarden voldoet kan en mag binnen RWS (en IenM) dat systeem niet de Rijkspas gebruiken.

1 Kaders Fysieke Beveiliging

De voor Rijkswaterstaat van toepassing zijnde wet- en regelgeving, kaders en richtlijnen liggen in verschillende documenten vast¹. De voor fysieke beveiliging relevante en geldende documenten staan hierna kort beschreven.

De van belang zijnde onderdelen uit die documenten zijn doorgevoerd in dit aansluitvoorwaarden document.

1.1 Rijksbrede kaders

Baseline Informatiebeveiliging Rijk (BIR): Regelt een gemeenschappelijk baselineniveau voor informatiebeveiliging binnen de rijksdienst. Stelt daarbij ook eisen aan de fysieke beveiliging (hoofdstuk 9), met name van systeemruimtes en rekencentra.

Kader Rijkstoegangsbeleid: Rijksbreed kader met betrekking tot het toegangsbeleid.

Normenkader beveiliging Rijkskantoren (NkBR): Rijksbreed normenkader voor kantoorgebouwen dat invulling geeft aan het kader Rijkstoegangsbeleid en het zoneringsmodel.

Zoneringsmodel: Model om tot een goede zonering van gebouwen te komen, gerelateerd aan te beschermen belangen.

Specifieke kaders voor havens (ISPS- 1.2.3.1. International Ship and Port Facility Security Code

Rijksbreed kader voor toepassing van Rijkspas:

Normenkader Rijkspas: bevatten de noodzakelijke, rijksbrede afspraken over uitgangspunten, processen, systemen, ontwerpen, specificaties en andere zaken die nodig zijn voor een succesvolle implementatie en een continue borging van kwaliteit en veiligheid.

1.2 IenM RWS kaders

Integraal beveiligingsbeleid IenM

Handboek Security: Het handboek security, onderdeel van de werkwijzer Aanleg en Onderhoud, is ontwikkeld om een duurzame en werkbare fysieke beveiliging te realiseren. Het is in die zin een uitwerking van de vigerende wet- en regelgeving op het gebied van fysieke beveiliging van objecten en kantoren.

CyberSecurity Implementatie Richtlijn-RWS (CSIR) is een vertaalslag en specifieke invulling van de relevante beheer doelen en beheersmaatregelen uit de BIR RWS en de NCSC Checklist beveiliging ICS/SCADA systemen voor de beveiliging van objecten RWS.

iStrategie beschrijft de RWS-brede doelen, de daaruit volgende IV-principes en aantal concrete maatregelen, waarmee standaardisatie en uniformiteit wordt nagestreefd. Daarbij wordt de structuur van de iStrategie Rijk gevolgd.

¹ Zie hiervoor het document "Overzicht kaders Integrale Beveiliging" door Patrick Dersjant (RWS CD CCIB)

Rijkswaterstaat Informatievoorziening Aansluitvoorwaarden (RIVA): geeft een overzicht van de te gebruiken ICT-producten en –bouwstenen.

Objectspecifieke kaders, zoals landelijke tunnel standaard.

2 Rijkspas

2.1 Rijkspas binnen RWS

De Rijkspas is een multifunctionele smartcard (gebruikt door alle op Rijkspas aangesloten departementen en agentschappen, centraal geproduceerd door Morpho) die wordt gebruikt als:

- Identiteitsbewijs binnen het Rijk (interdepartementale afspraak)
- Toegangsmiddel voor fysieke toegang binnen IenM (en mogelijk andere Rijksgebouwen)
- Mogelijk toegangsmiddel tot systemen (logische toegang)

Binnen RWS zijn 3 type Rijkspas in gebruik:

- Type P voor intern Personeel
- Type E voor Extern personeel (contract op naam)
- Type B voor Bezoekers (niet gepersonaliseerd)

Bij IenM (bestaande uit de beleidskern en de agentschappen zoals KNMI, ILenT en RWS) is de Rijkspas ingevoerd op basis van de interdepartementaal vastgelegde Normenkaders Rijkspas. De rijkspasprocessen zijn (en worden regelmatig) getoetst door de Auditdienst Rijk.

De uitgifte en het beheer van de Rijkspas is een gereguleerd proces, vergelijkbaar met de uitgifte van paspoorten en ID-kaarten, met een strenge verificatie van de gegevens en persoon aan wie een persoonlijke Rijkspas persoonlijk wordt verstrekt. Indien het recht op een Rijkspas verloopt (uit dienst) wordt de Rijkspas voor gebruik geblokkeerd en ingenomen.

2.2 Rijkspas systeemlandschap RWS

Binnen RWS (als onderdeel van IenM) zijn een aantal centrale systemen aanwezig die noodzakelijk zijn voor de Rijkspas keten en voldoen aan de rijksbreed vastgestelde Normenkaders Rijkspas.

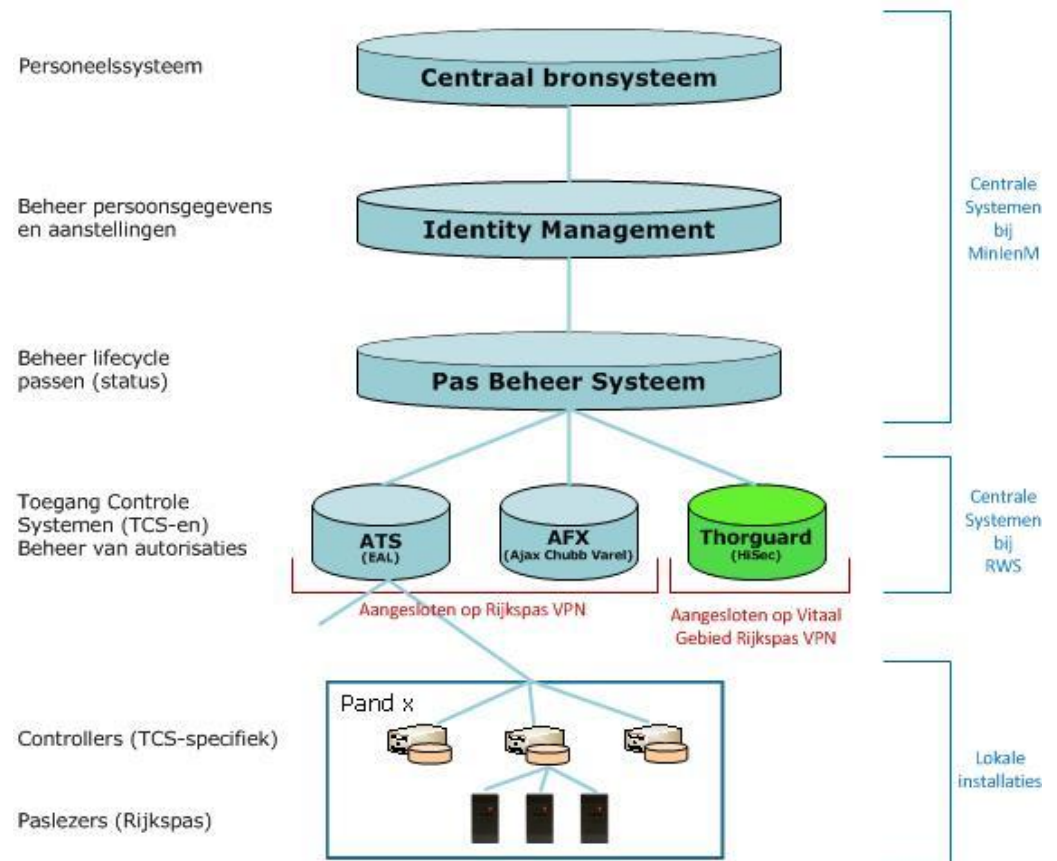
Deze systemen zijn in beheer bij CIV en voldoen aan de Rijkswaterstaat IV Aansluitvoorwaarden.

Component/systeem	Systeem-naam	Opmerking
Personeels- en aanstellings gegevens interne medewerkers	Bronstelsysteem: P-direkt	Centraal systeem van het Rijk voor de registratie van ambtenaren in rijks overheidsdienst
Identiteits- en aanstellingsgegevens alle medewerkers	Systeem: IdM	Centraal systeem met alle identiteits en aanstellingsgegevens van interne en externe medewerkers van IenM (en RWS)
Kaartbeheer Rijkspas	Systeem: PBS	Centraal kaartbeheer systeem dat de levenscyclus (status) van de Rijkspassen

Component/systeem	Systeem-naam	Opmerking
		beheerd, en van waaruit passen worden geproduceerd.
Toegangscontrole Systeem	TCS-en, 3 verschillende Rijkspas-aangesloten systemen binnen RWS beschikbaar en verplicht	Centrale RWS-toegangscontrole systeem, aangesloten op het centrale PBS. Hierin worden de autorisaties op de passen beheerd. Voor Vitaal Gebied Objecten (met infraclassificatie A) is één van deze TCS-en op een apart netwerk beschikbaar en verplicht
Lokale installaties	Via aansluiting op het RijkspasVPN worden lokale controllers aangesloten, die verbonden worden aan rijkspas-kaartlezers	Controllers en kaartlezers, die de uiteindelijke geautoriseerde werking van fysieke toegang verzorgen.

In onderstaand figuur staat dit schematisch weergegeven:

Rijkspas systeemlandschap RWS



3 Aansluitvoorwaarden Rijkspas

Voordat binnen het beheersgebied van RWS een uitvraag voor (Rijkspas) toegangscontrole systemen (TCS) wordt uitgebracht dient altijd contact te worden opgenomen met de Corporate Dienst (CD) van RWS.

Contactpersonen:

Erik Aartsen, clustercoördinator FE: erik.aartsen@rws.nl, tel 06 - 51000539

Henk van den Bos, adviseur, henk.vanden.bos@rws.nl, tel 06 - 10413184.

CD adviseert over het meest logische (vanuit beheersperspectief of vanuit infraclassificatie van een object) TCS om op aan te sluiten (bv steunpunt op naastliggend districtskantoor) en over de realisatie ervan, in samenwerking met Centrale Informatie Voorziening (CIV).

Een installatie dient voor het aansluiten op de RWS Rijkspas infrastructuur te voldoen aan de volgende voorwaarden.:

- Toegangscontrole Systeem
 - Er dient te worden gekoppeld aan één van de bestaande Rijkspas-aangesloten TCS-servers van RWS. Andere TCS-systemen worden niet toegestaan op het RWS-netwerk en kunnen en mogen geen gebruik maken van de Rijkspas.
- Controllers:
 - TCS-specifieke componenten, die dienen van de leverancier van het TCS betrokken te worden
- Kaartlezers
 - De kaartlezer dient door RijkspasBeheer en NBV getest en goedgekeurd te zijn.
 - De kaartlezer dient te kunnen worden uitgebreid met een SAM module, dit SAM module mag GEEN onderdeel vormen van de elektronica van de kaartlezer, maar dient te kunnen worden geplaatst in of in de directe nabijheid van de controller.
 - Die kaartlezer dient compatibel te zijn met het TCS waarop wordt aangesloten.
 - De communicatie tussen de leeseenheid en de controller dient op protocol basis plaats te vinden en te zijn encrypted op AES niveau met minimaal 256 bit.
- Plaatsen van hang- en sluitwerk bij de toegangscontrolepunten.
 - Het hang- en sluitwerk dient te voldoen aan NEN 5088 ,NEN 5089,EN 50133, EN 13633 en EN 13637 Het dient daarbij mogelijk te blijven om bij stroomuitval de toegangscontrolepunten (minimaal een calamiteiten route) met een sleutel te openen.
- Overige eisen:
 - Eventuele camerabeelden dienen minimaal 1 maand op locatie van het object realtime te worden opgeslagen op een digitale drager waarbij de aanwezige data geëxporteerd moeten kunnen worden naar een extern opslag medium volgens de laatste stand van de techniek, bv. solid state media.
 - De daarvoor geëigende deuren dienen (indien hier nog niet in is voorzien) te worden voorzien van een Standmelding, (Meldt onmiddellijk naar het TCS managementsysteem welke de deur te lang open is en het eventueel forceren van een deur)Bij een

brandalarm dienen alle binnendeuren te worden vrijgegeven indien deze zijn voorzien van dubbele kaartlezers. De periferie deuren blijven alleen vrij gegeven door de lokale NDO (groene Nood Deur Open drukker welke de vergrendeling spanningsloos maakt).

- o Alle onderdelen dienen minimaal 72 uur te kunnen doorwerken bij een primaire spanningsuitval.

- Eisen aan Oplevering:

- o De aannemer dient het gehele systeem in bedrijf te stellen en volledig te testen op de goede werking. Een en ander in nauw overleg met de projectleider van RWS, de leverancier van het TCS waaraan wordt gekoppeld en de functioneel beheerder (CD).
 - o Parameters voor de logische functies dienen door de TCS-leverancier te worden ingevuld en in principe eenmalig te worden ingevoerd.
 - o Bestandgegevens e.d. dienen door de gebruiker te worden ingevuld op de door de aannemer te leveren staten en in principe eenmalig te worden ingevoerd.
 - o Het vervaardigen en leveren van werktekeningen.
 - o Het vervaardigen van de benodigde kabellijsten.
 - o Het samenstellen en invullen van adreslijsten.
 - o Het vervaardigen en leveren van revisietekeningen, binnen 14 dagen na oplevering, en een logboek
 - o De "as build" revisietekeningen dienen ook de kabelloop weer te geven, zowel in pandig als eventueel buiten bekabeling.
 - o Het aanbieden van een Service Level Agreement (SLA) met een looptijd van 1 tot 3 jaar op de lokale componenten.
Voor de centrale componenten zijn centraal SLA afspraken gemaakt door CD.
- De aansluiting met het TCS (RijkspasKA of RijkspasVG, afhankelijk van de CS-box als het een object betreft) dient te worden aangevraagd bij CIV (Diederick Wolters – applicatie manager Rijkspas).
 - Het dopen van kaartlezers (voorzien van de Rijkspasleutels) kan en mag alleen gedaan worden door CD, na verificatie & validatie van de oplevering. Dit dient tijdig aangevraagd te worden bij Henk van den Bos of Frans Bosman.

4 Standaard apparatuur RWS Rijkspas

Binnen RWS zijn een aantal standaards voor apparatuur opgesteld, afwijken hiervan mag slechts na schriftelijke toestemming van RWS.

Voordat contact met leveranciers wordt opgenomen dient RWS CD (Henk van den Bos) op de hoogte te worden gesteld (henk.vanden.bos@rws.nl, tel 06-10413184).

Voor vragen rondom techniek kan contact op worden genomen met de adviseur beveiliging van CD, Frans Bosman, Frans.bosman@rws.nl, tel 06-53493695).

4.1 Toegangscontrole systemen

Er dient te worden aangesloten op een van de in de volgende tabel vermelde ToegangsControleSystemen. Koppeling met deze centrale systemen wordt gerealiseerd door aansluiting op het RijkspasVPN. Deze aansluiting dient aangevraagd te worden bij de CIV, die deze verbinding realiseert.

Voor objecten bepaalt het verplichte LocatieBeveiligingsPlan (opgesteld onder verantwoordelijkheid van de object-eigenaar) op basis van de CS-box (door bestuur RWS vastgestelde CyberSecurity-box, onderdeel van infraclassificatie) welk Rijkspas-regime geldend is: **bij CS-box A wordt RijkspasVG-Vitaal Gebied geëist, voor CS-box B (of lager) voldoet RijkspasKA (Kantoor Automatisering).**

Systeem	Leveranciersinformatie	Opmerking
ATS	EAL Contact: Pascal Vos Molenmakershoek 14 7328 JK Apeldoorn Tel: +31 55 5394900	
AFX	Chubb Fire & Security Contact: Hans Mesman Papendorpseweg 83 3528 BJ Utrecht Tel: +31 (0) 88 112 42 00	
ThorGuard	HISEC Contact: Robert Vavier Westlandseweg 16 A&B 2291 PG Wateringen +31 (0) 88 022 7300	Speciaal voor RijkspasVG, op apart VPN netwerk

4.2 Toegangscontrole componenten

De centrale operationele TCS-en dienen gekoppeld te worden via het aparte Rijkspas VPN netwerk met de lokale veldcomponenten voor toegangscontrole.

Aan de veldcomponenten worden de volgende eisen gesteld:

Component	Eis
Controller	<p>TCS-specifieke component waaraan de kaartlezers en deur-sturing aan gekoppeld is. De verschillende leveranciers gebruiken een eigen naamgeving voor deze componenten:</p> <ul style="list-style-type: none"> - ATS (EAL): Vossessoren - AFX (CFS): - TGMS (HISEC):
Kaartlezer	<p>De producent van de kaartlezer dient een NDA met RijkspasBeheer te hebben afgesloten en een SAM oplossing te kunnen bieden. De volgende producten kunnen gebruikt worden:</p> <ul style="list-style-type: none"> - EAL kaartlezers (specifiek voor gebruik bij ATS) - Deister kaartlezers
Tourniquets	<p>Indien anti-passback vereist wordt op de locatie, dient een-persoonstoegang gerealiseerd te worden. Voor kantoorlocaties met een bemensde receptie/beveiligingsbalie mogen lage tourniquets gehanteerd worden binnen de observatie-zone van de beveiligings/receptie loge.</p> <p>Indien een receptie/beveiligingsloge ontbreekt of buiten observatie zone dienen manshoge draaideuren of een-persoonssluizen gebruikt te worden.</p>

4.3 Hang- en Sluitwerk

Onderdeel	Norm	RWS standaard
Hang en sluitwerk algemeen	Het hang- en sluitwerk dient te voldoen aan NEN 5088, NEN 5089, EN 50133, 1-7, EN 13633 en EN 13637 Het dient daarbij mogelijk te blijven om bij stroomuitval de toegangscontrolepunten met een sleutel te openen.	Als aan norm wordt voldaan is er geen voorkeur voor leverancier.
elektrisch veiligheidsslot, smal, enkelzijdig krukgestuurd	Electronic Lock, nachtschoot dient automatisch bij sluiten van deur vergrendelen. Zie ook algemeen hang en sluitwerk	RWS standaard is ASSA Abloy EL460
elektrisch veiligheidsslot, smal, dubbelzijdig krukgestuurd	Electronic Lock, nachtschoot dient automatisch bij sluiten van deur vergrendelen. Zie ook algemeen hang en sluitwerk	RWS standaard is ASSA Abloy EL461
elektrisch veiligheidsslot, breed, enkelzijdig krukgestuurd	Electronic Lock, nachtschoot dient automatisch bij sluiten van deur vergrendelen. Zie ook algemeen hang en sluitwerk	RWS standaard is ASSA Abloy EL560
elektrisch veiligheidsslot, breed dubbelzijdig krukgestuurd	Electronic Lock, nachtschoot dient automatisch bij sluiten van deur vergrendelen. Zie ook algemeen hang en sluitwerk	RWS standaard is ASSA Abloy EL561
Niet-elektrische sloten	hang en sluitwerk klasse extra zwaar	Als aan norm wordt voldaan is er geen voorkeur voor leverancier.
Vluchtbar	Met signalering	Als aan norm wordt voldaan is er geen voorkeur voor leverancier.
Nood Deur Opener	Groen met dubbele contacten uitgevoerd	Als aan norm wordt voldaan is er geen voorkeur voor leverancier.
Hangslot	Zie algemeen hang en sluitwerk	Voorkeur RWS: ASSA Abloy veiligheidshangslot type PL362/25KN/KD
Bijzetslot	Klasse zwaar RVS inclusief sluitkom	Voorkeur RWS: ASSA Abloy 5019C
Securistrip		Als aan norm wordt voldaan is er geen voorkeur voor leverancier.

5 Standaard inrichtingen RWS panden met Rijkspas

In bijgaande tabel staat vermeld op welke manier de huidige locaties met Rijkspas worden beveiligd.

De categorisering volgens het sturingsmodel Gebouwen wordt gehanteerd:

A Hoofdvestigingen

B Districtskantoren

C Steunpunten

D loodsen (meestal op terrein van een van bovenstaande)

E Verkeerscentrales

G Infra objecten

Indien in onderstaande tabel O staat, betekent dat optionele Extra functionaliteit, niet volgens de huidige standaard inrichting.

	A: hoofdkantoren	B: districtskantoren	C: steunpunten	D: loodsen	E/G: Objecten (afh van risico classificatie)
Hekwerk om terrein	O	O	Ja	Ja	Ja
Toegangshek: electr. Rolpoort	O	O	Ja	O	Ja
Toegangshek op Rijkspas	O	O	ja	O	Ja
Slagboom	Ja	O	O	-	-
Eventuele slagboom op Rijkspas	ja	ja	Ja	Ja	Ja
Ingang kantoor/object op Rijkspas	Ja	ja	ja	O	Ja
In/uit lezing (anti-passback)	ja	O	Nee	Nee	Ja
Gezoneerde ruimte (IT/MER) op Rijkspas	Ja	Ja	O	-	Ja
Inbraak systeem	Ja	Ja	Ja	O	Ja
Alarmschakeling in/uit op Rijkspas	O	O	Ja	O	O
Intercom bij hek	Ja	O	Ja	Nee	Ja

Voor de kantoorlocaties type A t/m D geldt het Corporate Beveiligings Model voor de te nemen maatregelen (OBE - Organisatorisch, Bouwkundig en Elektronisch).

Voor objecten geldt hiervoor het Handboek Security. De benodigde maatregelen voor (keten van) objecten is afhankelijk van de risicoclassificatie van het object.