Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Aansluitvoorwaarden Rijkspas RWS

Versie 1.6

Datum Maart 2021
Status Definitief

Colofon

CD
Dir. Facilitair en Financiën

Griffioenlaan 2 Utrecht

Contact RWS CD – DFF – FM – team Fysieke Beveiliging
E-mail: rijkspas@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
1.5	5-12-2016	Henk van den Bos	- Speciale versie voor CDV
1.6	21-2-2021	Peter Stolk / Barry van Veen	- Div. updates verwerkt

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) 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 Rijkspasbeheer
- Ketentest Rijkspas door IenW en RWS
- Toets beheermodel applicaties door RWS-CIV

In dit document wordt beschreven op welke wijze en onder welke voorwaarden panden binnen het verzorgingsgebied van Rijkswaterstaat 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 dit 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 vast. De voor fysieke beveiliging relevante en geldende documenten staan hierna kort beschreven.
De van belang zijnde onderdelen uit die documenten zijn doorgevoerd in dit document.

1.1 Rijksbrede kaders

Baseline Informatiebeveiliging Overheid (BIO): Regelt een gemeenschappelijk baselineniveau voor informatiebeveiliging binnen de rijksdienst. Stelt daarbij ook eisen aan de fysieke beveiliging (hoofdstuk 11).

Normenkader beveiliging Rijkskantoren (NkBR): Rijksbreed normenkader voor Rijks(verzamel)kantoren dat invulling geeft aan de fysieke beveiligingsmaatregelen op en om Rijks(verzamel)kantoren.

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 IenW RWS kaders

Integraal beveiligingsbeleid IenW

Handboek Security: Het handboek security, onderdeel van de werkwijzer Aanleg en Onderhoud, is ontwikkeld om een duurzame en werkbare fysieke beveiliging te realiseren.

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

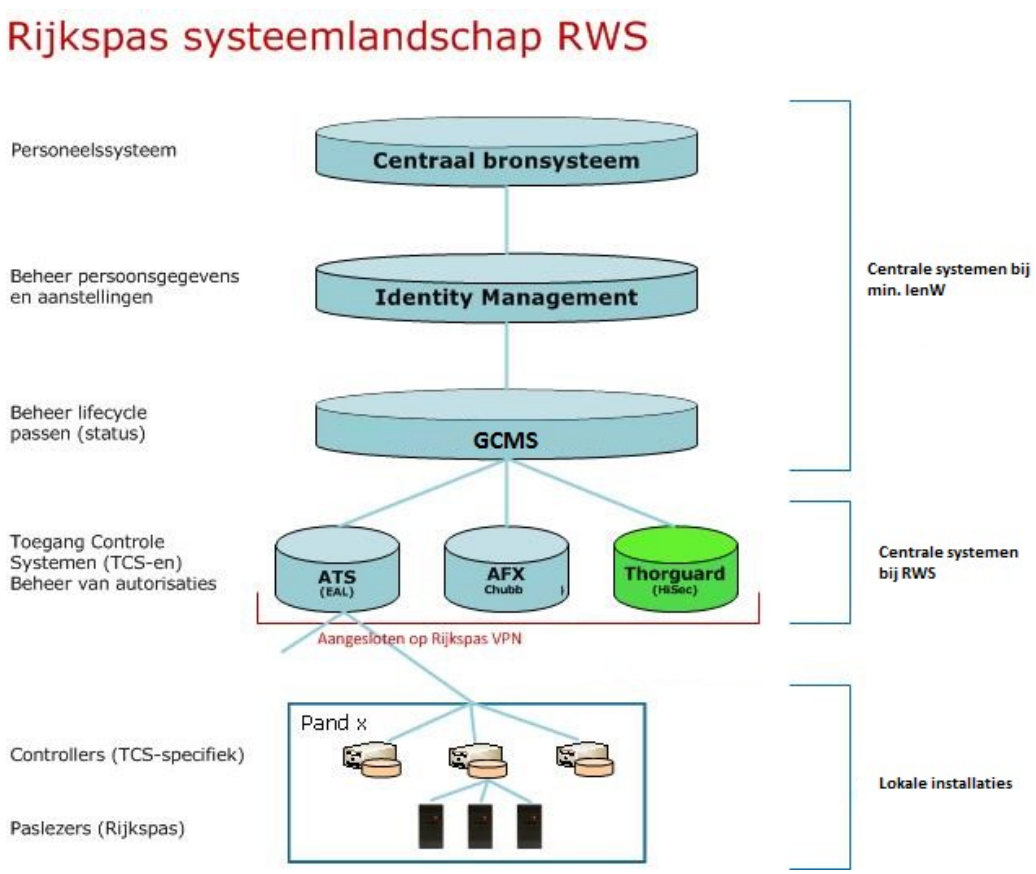
2 Rijkspas

2.1 Rijkspas systeemlandschap RWS

Binnen RWS 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	Bronsysteem: P-direkt	Centraal systeem van het Rijk voor de registratie van ambtenaren in rijksoverheidsdienst
Identiteits- en aanstellingsgevens alle medewerkers	Systeem: IdM	Centraal systeem met alle identiteits en aanstellingsgegevens van interne en externe medewerkers van IenM (en RWS)
Generiek Card Management Systeem	Systeem: GCMS	Centraal kaartbeheer systeem dat de levenscyclus (status) van de Rijkspassen 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 GCMS. Hierin worden de autorisaties op de passen beheerd.
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 het figuur op de volgende pagina staat dit schematisch weergegeven.


Rijkspas systeemlandschap RWS
Personeelssysteem
Centraal bronsysteem
Beheer persoonsgegevens en aanstellingen
Identity Management
Beheer lifecycle passen (status)
GCMS
Centrale systemen bij min. IenW
Toegang Controle Systemen (TCS-en) Beheer van autorisaties
ATS (EAL)
AFX Chubb
Thorguard (HiSec)
Centrale systemen bij RWS
Aangesloten op Rijkspas VPN
Pand x
Controllers (TCS-specifiek)
Paslezers (Rijkspas)
Lokale installaties

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 team fysieke beveiliging van DFF – FM – RWS CD via rijkspas@rws.nl.

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 getest en goedgekeurd te zijn.
  - Het systeem, kaartlezer en controller moeten voorzien zijn van 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. Deze combinatie moet met de speciale SAM doopkaart van Rijkspasbeheer gedoopt kunnen worden.
  - 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:
  - 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).
  - Alle onderdelen dienen minimaal 72 uur te kunnen doorwerken bij een primaire spanningsuitval.

- Eisen aan Oplevering:
    - 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).
    - Parameters voor de logische functies dienen door de TCS-leverancier te worden ingevuld en in principe eenmalig te worden ingevoerd.
    - 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.
    - Het vervaardigen en leveren van werktekeningen.
    - Het vervaardigen van de benodigde kabellijsten.
    - Het samenstellen en invullen van adreslijsten.
    - Het vervaardigen en leveren van revisietekeningen, binnen 14 dagen na oplevering, en een logboek
    - De “as build” revisietekeningen dienen ook de kabelloop weer te geven, zowel inpandig als eventueel buiten bekabeling.
    - 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 dient te worden aangevraagd bij CIV (Diederick Wolters – applicatie manager Rijkspas).
- Het dopen van kaartlezers (voorzien van de Rijkspassleutels) kan en mag alleen gedaan worden team fysieke beveiliging, na verificatie & validatie van de oplevering. Dit dient tijdig aangevraagd te worden via rijkspas@rws.nl.

4 Standaard apparatuur RWS Rijkspas

4.1 Toegangscontrole systemen

Alleen één van in de onderstaande tabel vermelde Toegangscontrole Systemen kunnen worden aangesloten binnen het verzorgingsgebied van RWS CD. 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.

Systeem	Leveranciersinformatie
ATS	EAL Contact: Pascal Vos Molenmakershoek 14 7328 JK Apeldoorn Tel: +31 55 5394900
AFX	Chubb Fire & Security Contact: André Vermeij 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

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	TCS-specifieke component waaraan de kaartlezers en deur-sturing aan gekoppeld is. De verschillende leveranciers gebruiken een eigen naamgeving voor deze componenten: - ATS (EAL): Vossessoren - AFX (CFS): - TGMS (HISEC):
Kaartlezer	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: - EAL kaartlezers (specifiek voor gebruik bij ATS) - Deister kaartlezers
Tourniquets	Indien anti-passback vereist wordt op de locatie, dient een-persoonstoegang gerealiseerd te worden.

4.3 Hang- en Sluitwerk

Onderdeel	Norm
Hang en sluitwerk alge-meen	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.
elektrisch veiligheidsslot	Een kruk gestuurd solenoid slot met automatische nachtschoot uitwerper zoals de AssaAbloy EL serie of gelijkwaardig.
Niet-elektrische sloten	hang en sluitwerk klasse extra zwaar
Vluchtbar	Met signalering
Nood Deur Opener	Groen met dubbele contacten uitgevoerd
Hangslot	Zie algemeen hang en sluitwerk
Bijzetslot	Klasse zwaar RVS inclusief sluitkom
Secustrip	Anti-inbraak strip voor deuren

Let op: De bovenstaande tabel verwijst alleen naar het noodzakelijke hang- en sluitwerk. Uiteraard dient de gehele gevel te voldoen aan het vereiste weerstandsniveau zoals beschreven in het locatiebeveiligingsplan of de risico analyse van de betreffende locatie.