

Richtlijn digitale gegevensstromen



Afdeling: ICT Expertisecentrum

Datum: 18-11-2024

Auteur: Bas Rabeling

Versie: 2.0

Wijzigingshistorie

VERSIE	DATUM	AUTEUR	OMSCHRIJVING	VERZONDEN AAN	STATUS
1.0	04/07/2023	Bas Rabeling	Document definitief gemaakt	DWO	Final
1.1	18/07/2023	Bas Rabeling	Update in verband met risico's OpenTunnel	DWO	Final
1.2	29/08/2023	Bas Rabeling	Update 4, 6 en 10	DWO	Final
1.3	31/08/2023	Bas Rabeling	Update 7	DWO	Final
1.4	25/10/2023	Bas Rabeling	Update 10	DWO	Final
1.5	1/12/2023	Bas Rabeling	Punt 15 toegevoegd	DWO	Final
1.6	24/4/2024	Bas Rabeling	Punt 6 en 11 toegevoegd	DWO	Final
1.7	17/10/2024	Bas Rabeling	Punt 3 toegevoegd, Punt 8 aangepast	DWO	Final
1.8	13/11/2024	Bas Rabeling	Punt 3 verduidelijkt	DWO	Final
2.0	18/11/2024	Bas Rabeling	Document vastgesteld	DWO	Final

Goedkeuringshistorie

VERSIE	DATUM	AUTORISATIE	J/N	TOELICHTING
1.0	04/07/2023	Walter van Oostrum	J	
2.0	18/11/2024	Walter van Oostrum	J	

Bijlagen en verwijzingen

VERSIE	DATUM

Inhoudsopgave

Inleiding	4
1. Uitgangspunten	4
Bijlage 1: Links	8

Inleiding

Het CAK moet voldoen aan de Baseline Informatie Beveiliging overheid (BIO). Hieruit volgen ook de verplichte normen vanuit het forum standaardisatie. Dit document beschrijft de richtlijnen voor digitale gegevensstromen binnen het CAK en voor inkomende- en uitgaande gegevensstromen. Hierbij zijn de BIO en de verplichte normen vanuit het forum standaardisatie als uitgangspunt genomen.

1. Uitgangspunten

Security hanteert de volgende uitgangspunten met betrekking tot gegevensstromen binnen het CAK:

Encryptie en versleuteling

1. Al het verkeer tussen en binnen zones binnen het CAK domein verloopt versleuteld, tenzij er geen veilig protocol voor beschikbaar is.
2. Al het verkeer tussen het CAK en de buitenwereld verloopt versleuteld, tenzij er geen veilig protocol voor beschikbaar is.
3. Vanaf Basis Beveiligingsniveau 2 (BBN2) geldt dat wanneer er geen sprake is van end-to-end encryptie dat de inhoud van het berichtenverkeer zelf versleuteld moet worden tenzij dit vanwege afgesproken standaarden met ketenpartners niet mogelijk is. Dit voorkomt dat de berichten leesbaar zijn in queues of door de leverancier van externe gateway oplossingen kunnen worden ingezien. Dit geldt zowel voor berichtenverkeer binnen het CAK als voor verkeer dat naar buiten gaat.
4. Versleuteling vindt plaats door middel van encryptie algoritmes en ciphers die door het Nationaal Cyber Security Center (NCSC) minimaal als voldoende zijn aangemerkt.

Integriteit

5. Wanneer er gebruik gemaakt wordt van elektronische handtekeningen dan moet vanaf Basis Beveiligingsniveau 2 (BBN2) gebruik gemaakt van de AdES Baseline Profile standaard. De AdES Baseline Profiles moeten worden toegepast op de ondertekening van XML-, CMS-, PDF- en ZIP-bestanden met geavanceerde en/of gekwalificeerde elektronische handtekeningen, zegels of tijdstempels. Het gebruik van elektronische handtekeningen kan een mitigerende maatregel zijn die voort komt uit een aanvullende risico analyse.

Inspectie en afhandeling van verkeer tussen zones

6. Al het verkeer dat zich tussen netwerkzones verplaatst ondergaat pakket inspectie middels een Intrusion Prevention Systeem(IPS).
7. De ontsluiting van webapplicaties die door het CAK worden gehost en vanuit een andere zone worden benaderd moet via de Webapplication Firewall verlopen. Denk hierbij bijvoorbeeld aan interne webapplicaties die worden ontsloten naar een VDI of aan een intern gehoste webapplicatie die wordt ontsloten naar het internet.

Berichtenverkeer van en naar buiten

8. Wanneer BBN2 data wordt uitgewisseld dan moet inkomend berichtenverkeer tussen systemen over het internet gaan via een centrale gateway. Zodat security eisen centraal kunnen worden afgedwongen. Uitgaand verkeer moet worden afgestemd met data-architectuur (CIO Office).
9. Autorisatie en authenticatie op alle API's/tunnels van de centrale gateway moet worden ingericht met behulp van OAuth2 en OpenID connect. Wanneer dit niet is ingericht mag de gateway alleen vanuit de ESB worden benaderd.
10. Berichtenverkeer naar buiten mag alleen vanuit servers vanuit vertrouwde netwerksegmenten worden opgezet;
11. De IAAS cloudomgevingen en on-premise omgevingen van het CAK hebben hun eigen centrale gateway en CAK firewall.
12. Authenticatie op SFTP verbindingen moet worden ingericht met Public Key Authentication.

Berichtenverkeer tussen SaaS diensten

13. Berichtenverkeer tussen SaaS diensten waarbij er sprake is van de uitwisseling van BBN2 data mag op 2 manieren worden ingeregeld:

- Via een door het CAK beheerde omgeving. Dit biedt het CAK de volgende mogelijkheden:
 - a. Inspectie van het verkeer tussen de SaaS diensten;
 - b. Het controleren van de beveiliging van de uitwisseling;
 - c. Het kunnen stopzetten van de uitwisseling mocht een SaaS dienst gecompromitteerd zijn.
- Een rechtstreekse koppeling tussen 2 SaaS diensten, wanneer aan de onderstaande voorwaarden kan worden voldaan:
 - a. Beide partijen moeten beschikken over een ISO27001 met verklaring van toepasbaarheid en een SOC2 type II verklaring en deze beschikbaar stellen aan het CAK;
 - b. De beveiliging en authenticatie van de verbinding moet aantoonbaar voldoen aan de encryptie en authenticatie eisen uit deze richtlijn (zie 3,12 en 14);
 - c. Er moet worden vastgelegd welk van de partijen verantwoordelijk is voor de verbinding;
 - d. Er moet worden vastgelegd welk van de partijen het CAK moet benaderen om de uitwisseling per direct stop te kunnen zetten;
 - e. Beide partijen moeten voldoen aan NIS2 op de ingangsdatum hiervan;
 - f. Het moet mogelijk zijn om realtime logging van de uitwisseling naar het SIEM van het CAK te sturen.

Authenticatie en rechten API's

14. Interne API's moeten op dezelfde wijze worden beschermd als externe benaderbare API's;
15. Autorisatie en authenticatie op API's moet worden ingericht met behulp van OAuth2 en OpenID connect;
16. Single Sign On functionaliteit mag zowel met OpenID Connect als met SAML2 worden gerealiseerd;
17. De rechten van API's moeten worden ingeregeld op basis van Least privilege. Dit wil zeggen dat API's de minimale rechten krijgen die ze nodig hebben.
18. API's mogen alleen via een API Gateway beschikbaar worden gesteld. Op deze manier kan de beveiliging centraal worden ingeregeld en is deze ook controleerbaar.

Standaarden

19. Het CAK voldoet aan verplichte standaarden van forum standaardisatie.
20. Voor OAuth 2.0 implementaties moet worden voldaan aan het NL GOV Assurance profile for OAuth 2.0.
21. Voor SAML2.0 implementatie zijn de volgende standaarden van toepassing;
22. Voor OIDC wordt gewerkt aan het NL GOV Assurance Profile for OIDC wanneer deze verplicht wordt gesteld moet hier aan worden voldaan.
23. Voor het gebruik van elektronische handtekeningen moet vanaf BBN2 gebruik gemaakt worden van de AdES Baseline Profile standaard.

Bijlage 1: Links

Titel	Link
AdES baseline profiles	https://www.forumstandaardisatie.nl/open-standaarden/ades-baseline-profiles
Forum standaardisatie	https://www.forumstandaardisatie.nl
NL GOV Assurance profile for OAuth 2.0	https://forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20
NL GOV Assurance Profile for OIDC	https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oidc
SAML2 standaard	https://www.forumstandaardisatie.nl/open-standaarden/saml