Gemeente Amsterdam

Versie: 1.0
Datum:08 februari 2019
Onderwerp: Scanvoorziening incl. Digitaal PostverwerkingsSysteem gemeente Amsterdam
Betreft: Bijlage Privacy, Security en BIG
Inkoopcode: AICT-2018-0016

Bijlage Privacy, Security en BIG

Inleiding
In deze bijlage staan eisen in het kader van Privacy, Security en aanvullingen op de BIG beschreven die de gemeente Amsterdam stelt aan de gevraagde opdracht. Inschrijver dient te voldoen aan de gunningseisen zoals beschreven in dit document.
Deze bijlage maakt integraal onderdeel uit van de Aanbestedingsleidraad en daarvan dient een Inschrijver kennis te hebben vernomen.

Inhoud

1 Informatiebeveiliging

1.1 Eisen ten aanzien van encryptie

Ten aanzien van encryptie heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van encryptie
1.	Inschrijver voorziet in encryptie van de interne HDD/SSD van de scanapparatuur, waaronder minimaal de volgende data wordt versleuteld: adresboek, authenticatiegegevens gebruikers, (tijdelijk) opgeslagen documenten, logs, network interface settings en configuratie. De encryptiestandaard is minimaal AES 256.
2.	Inschrijver garandeert dat de (embedded) data encryptie systeem/module van de Scanapparatuur FIPS140-2 is gevalideerd.

1.1 Eisen ten aanzien van de integriteit

Ten aanzien van de integriteit dienen de volgende eisen in acht genomen te worden:

Nr	Eisen ten aanzien van de integriteit
3.	Inschrijver dient ervoor te zorgen dat authenticatie van systemen voor servers minimaal plaatsvindt op basis van IP (ACL) en DNS resolutie. Voor cliënt systemen vindt authenticatie plaats op basis van IP (ACL).
4.	Inschrijver dient ervoor te zorgen dat de Scanvoorziening een controlemechanisme heeft waarmee transactie- en verwerkingsfouten kunnen worden gedetecteerd en gegevens consistent zijn.
5.	Inschrijver dient ervoor te zorgen dat de Scanvoorziening een controlemechanisme heeft /ondersteunt waarmee data-uitwisseling met andere systemen gecontroleerd kan worden op mutaties tijdens het transport (CRC controle).
6.	Inschrijver dient ervoor te zorgen dat toegang van een systeem of een systeemoplossing een uniek inlogaccount heeft.
7.	Inschrijver dient ervoor te zorgen dat iedere gebruiker (inclusief beheerders) een uniek persoonlijk inlogaccount heeft.
8.	Inschrijver dient ervoor te zorgen dat indien er (herleidbare) persoonsgegevens langer dan 6 maanden bewaard worden, daar een specifieke melding van wordt gedaan bij de privacy functionaris van Amsterdam.
9.	Inschrijver dient ervoor te zorgen dat inkomende digitale data gecontroleerd wordt op malafide code/Virussen/Trojans/Spam.
10.	Inschrijver dient ervoor te zorgen dat wanneer data-uitwisseling met andere systemen over het WAN plaatsvindt, encryptie wordt toegepast. De datastroom van de scanner naar de server valt hierbuiten.
11.	Inschrijver garandeert dat alle data die wordt verwerkt binnen het domein van de gemeente Amsterdam blijft.

1.2 Eisen ten aanzien van de vertrouwelijkheid

Ten aanzien van de vertrouwelijkheid dienen de volgende eisen in acht genomen te worden:

Nr	Eisen ten aanzien van de vertrouwelijkheid
12.	In het door Inschrijver aangeboden DPS dient data afgeschermd te zijn d.m.v. toegangscontrole en encryptie.
13.	In het door Inschrijver aangeboden DPS dient transport binnen de systeem oplossing geëncrypt te zijn op applicatie-niveau.

Nr	Eisen ten aanzien van de vertrouwelijkheid
14.	Op het door Inschrijver aangeboden DPS dient transport op het LAN geëncrypt te zijn op applicatie-niveau met een certificaat autoriteit.
15.	Op het door Inschrijver aangeboden DPS dient data gescheiden te worden van de applicaties op netwerkniveau.
16.	Op het door Inschrijver aangeboden DPS dient er een firewall op de workstations te worden toegepast.

1.2 Eisen ten aanzien van logische toegangscontrole

Ten aanzien van logische toegangscontrole heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van logische toegangscontrole
17.	Inschrijver dient ervoor te zorgen dat authenticatie-informatie wordt opgeslagen d.m.v. een veilige hash.
18.	Inschrijver past het beleid van de gemeente Amsterdam rondom wachtwoorden toe: • Een wachtwoord verloopt elke 90 dagen; • Minimaal 8 tekens lang; • Ten minste 1 kleine letter bevatten; • Ten minste 1 hoofdletter bevatten; • Ten minste 1 cijfer bevatten; • Ten minste 1 speciaal teken bevatten; • Moet versleuteld worden opgeslagen; • Wordt niet op het scherm getoond tijdens het ingeven.
19.	Inschrijver garandeert ten aanzien van gebruikers authenticatie dat er een account lock-out policy ingesteld kan worden.
20.	Inschrijver dient ervoor te zorgen dat authenticatie van personen plaats vindt door middel van een wachtwoord of door middel van het aansluiten op een centrale authenticatie faciliteit van de gemeente Amsterdam
21.	Inschrijver garandeert als authentication mode de toepassing van netwerk authenticatie (geen lokale authenticatie).
22.	Inschrijver voorziet de scanapparatuur van ID card authentication: card/pin authenticatie (2FA).
23.	Inschrijver garandeert dat restricties kunnen worden toegekend aan groepen gebruikers geregistreerd op de authenicatieserver (netwerk autorisatie in combinatie met groepautorisatie).
24.	Inschrijver garandeert dat het instellen van gebruikersautorisaties uitsluitend geschiedt via een administratorfunctie (let op: instellen is niet toekennen/bepalen/vaststellen).
25.	Inschrijver garandeert dat session management mogelijk is op de Scanapparatuur (Automatisch “locken” wanneer deze een bepaalde tijd niet wordt gebruikt).
26.	De Opdrachtnemer dient, uitsluitend op locatie waar de Scanvoorziening staat, software te installeren op de Scanvoorziening. Remote login op de Scanvoorziening is niet toegestaan.
27.	Binnen de door Inschrijver aangeboden Scanvoorziening kan een vastgesteld autorisatieschema (op basis van rollen of profielen) ingevoerd worden, dat bepaalt welke gebruikers met welke rechten toegang hebben tot welke informatie en welke taken zij kunnen uitvoeren.
28.	Inschrijver dient ervoor te zorgen dat autorisaties plaatsvinden op basis van individuele personen.

1.3 Eisen ten aanzien van logging

Ten aanzien van logging heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van logging
29.	Inschrijver garandeert dat auditlogs aanwezig zijn of aangemaakt kunnen worden voor login, machine, netwerkverkeer en handelingen scanoperator. Alle mutaties, systeemgebeurtenissen en beheeractiviteiten met betrekking tot instellingen, documenten en metadata, alle configuratie van systeem- functionaliteit en alle configuratie van ingevoerde schema's/regimes moeten geautomatiseerd kunnen worden gedocumenteerd (datalog).
30.	Inschrijver dient ervoor te zorgen dat alle inlogpogingen (inclusief mislukte) van gebruikers en systemen worden gelogd. Hierbij wordt minimaal het volgende in de log vastgelegd: • De accountnaam; • De locatie; • Het tijdstip; • Het resultaat van de inlogpoging.
31.	Inschrijver garandeert de aanwezigheid van functionaliteit om logs (gebruiksvriendelijk) te beheren en analyseren.
32.	Inschrijver dient logregels te genereren die minimaal de volgende gegevens bevatten: • Een tot een natuurlijk persoon herleidbare gebruikersnaam/ID of system ID; • De gebeurtenis; • Waar mogelijk de identiteit van het werkstation of de locatie; • Het object waarop de handeling werd uitgevoerd; • Het resultaat van de handeling; • De datum en het tijdstip van de gebeurtenis.
33.	Inschrijver garandeert dat in een log-regel in geen geval gevoelige gegevens worden opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden).
34.	Inschrijver moet de loggings kunnen presenteren, zodanig dat een specifieke gebeurtenis kan worden geïdentificeerd en gereconstrueerd.
35.	Inschrijver garandeert dat als de opslaglocatie van het datalog haar opslagcapaciteit dreigt te overschrijden, hier melding van gemaakt wordt door het systeem aan de applicatiebeheerder.
36.	Inschrijver garandeert dat de volgende gebeurtenissen in ieder geval worden opgenomen in de logging: • Gebruik van technische en functioneel beheerfuncties; • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels; • Beveiligingsincidenten; • Verstoringen in het productieproces; • Handelingen van gebruikers.
37.	Inschrijver garandeert dat het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
38.	De door Inschrijver aangeboden Scanvoorziening voorziet in beperkte toegang (uitsluitend leesrechten) tot de logbestanden. Deze toegang is uitsluitend voor daarvoor geautoriseerde gebruikers.
39.	Inschrijver garandeert dat logbestanden zodanig worden beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
40.	Inschrijver dient ervoor te zorgen dat de Administrator van de Scanvoorziening de configuratie (instellingen) van de logging moet kunnen bewerken, opdat kan worden geselecteerd welke gegevens automatisch worden opgeslagen.

Nr	Eisen ten aanzien van logging
41.	Inschrijver dient ervoor te zorgen dat alle logbestanden minimaal 180 dagen worden bewaard.
42.	Inschrijver dient te garanderen dat iedere wijziging in de configuratie van het datalog automatisch wordt geregistreerd en vastgelegd.
43.	Inschrijver dient te garanderen dat de aangebrachte wijzigingen in de configuratie van het datalog niet leiden tot mutatie van de gegevens die reeds in het datalog zijn opgeslagen.
44.	De door Inschrijver aangeboden Scanvoorziening moet de logging kunnen exporteren naar een andere omgeving waar de logs kunnen worden opgeslagen en bewaard.
45.	Inschrijver dient ervoor te zorgen dat de logs voor authenticatie en transport ten minste lokaal op het systeem op een beveiligde locatie (met zoveel als mogelijk alleen leesrechten toegepast) worden opgeslagen en samen met de overige data kunnen worden meegenomen in de back-up. Logbestanden hebben een duidelijke structuur waardoor rapportages kunnen worden samengesteld op basis van de inhoud van het logbestand.
46.	Inschrijver dient ervoor te zorgen dat alle data-uitwisselactiviteiten via de systeemkoppelingen, worden gelogd. Hierbij wordt minimaal het volgende in de log vastgelegd: • De accountnaam (welk systeem); • Het tijdstip; • Het soort data; • Het transportnummer; • Het resultaat van de uitwisseling.
47.	De door Inschrijver aangeboden Scanvoorziening moet gebruik maken van een tijdsynchronisatie bron.

1.4 Eisen ten aanzien van de beveiliging van papieren documenten

Ten aanzien van de beveiliging van papieren documenten heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van de beveiliging van papieren documenten
48.	Voor de door Inschrijver aangeboden Scanapparatuur is printen als functionaliteit niet toegestaan, danwel beveiligd te blokkeren voor gebruikers (disabled).
49.	Voor de door Inschrijver aangeboden Scanapparatuur is kopieeren als functionaliteit niet toegestaan, danwel beveiligd te blokkeren voor gebruikers (disabled).
50.	Voor de door Inschrijver aangeboden Scanapparatuur is faxen (send en receive) als functionaliteit niet toegestaan, danwel beveiligd te blokkeren voor gebruikers (disabled).
51.	Voor de door Inschrijver aangeboden Scanapparatuur geldt dat hierop unauthorized copy control kan worden ingesteld (= indien de scanapparatuur de mogelijkheid tot printen heeft, dan kunnen de geprinte/gekopieerde documenten worden voorzien van een security watermark pattern of text stamp, waarmee print/kopie is te herleiden naar gebruiker/machine/tijdstip).
52.	Voor de door Inschrijver aangeboden Scanapparatuur geldt dat hierop locked print kan worden ingesteld (= indien de scanapparatuur de mogelijkheid tot printen heeft, dan kan printen pas plaatsvinden na authenticatie gebruiker)

1.5 Eisen ten aanzien van operating security

Ten aanzien operating security heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van operating security
53.	Voor de door Inschrijver aangeboden Scanapparatuur kan operational panel lock worden ingesteld (= toegang tot gebruikersfuncties is te blokkeren op grond van security overwegingen)

1.6 Eisen ten aanzien van inbreuken op de beveiliging

Ten aanzien van inbreuken op de beveiliging heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van inbreuken op de beveiliging
54.	Voor de door Inschrijver aangeboden Scanapparatuur geldt dat firmware updates digitaal zijn ondertekend.
55.	Voor de door Inschrijver aangeboden Scanapparatuur is softwareverificatie van beveiligingsfuncties vereist. Dit wordt gebruikt om te verifieren of beveiligingsfuncties niet gewijzigd zijn en naar behoren functioneren.
56.	Inschrijver garandeert (indien van toepassing) dat de Scanvoorziening voldoet aan de Open Web Application Security Project (OWASP) richtlijnen. Zie Bijlage: [OWASP_Top_10-2017_(en).pdf].
57.	De Inschrijver van de aangeboden scanapparatuur toont aan productcertificatie security features obv ISO/IEEE 15408 (common criteria) in combinatie met IEEE 2600.2 Standard Protection Profile for Hardcopy Devices.

1.7 Eisen ten aanzien van onderhoud en service

Ten aanzien onderhoud en service heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van onderhoud en service
58.	Opdrachtnemer past secure repair access toe bij onderhoud en service.
59.	Opdrachtnemer dient te voorzien in cleansing services. Daarbij wordt alle identificerende informatie van een machine verwijderd voordat (onderdelen van) het apparaat de lokatie verlaten. Denk hierbij aan informatie opgeslagen in geheugen (adresboek, netwerkadressen), labels/stickers met afdelingsnamen, servicedeskinformatie, etc.
60.	Opdrachtnemer biedt geen externe cloud/Software-as-a-Service-oplossing aan (externe cloud/SaaS niet toegestaan).
61.	Inschrijver garandeert dat de toegangsrechten van zijn medewerkers het mogelijk maken om werkzaamheden op de server te verrichten zonder daarbij data in te zien en/of te wijzigen van de gemeente Amsterdam of administrators tekenen persoonlijk een integriteitsverklaring van de gemeente Amsterdam.

1.8 Eisen ten aanzien van netwerkbeveiliging

Ten aanzien van netwerkbeveiliging heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van netwerkbeveiliging
62.	Inschrijver voorziet in de mogelijkheid om binnenkomend dataverkeer te whitelisten (mag alleen afkomstig zijn van vooraf geïdentificeerde IP-adressen)

Nr	Eisen ten aanzien van netwerkbeveiliging
63.	Inschrijver maakt het mogelijk dat uitsluitend vereiste poorten kunnen worden gebruikt voor dataverkeer. Overige poorten kunnen worden afgesloten.
64.	Voor de door Inschrijver aangeboden Scanapparatuur is e-mailen (send en receive) als functionaliteit niet toegestaan, danwel beveiligd te blokkeren voor gebruikers (disabled).
65.	Voor de door Inschrijver aangeboden Scanapparatuur is wifi als functionaliteit niet toegestaan, danwel beveiligd te blokkeren voor gebruikers (disabled).

1.9 Eisen ten aanzien van hardwarebeveiliging

Ten aanzien van hardwarebeveiliging heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van hardwarebeveiliging
66.	Voor de door Inschrijver aangeboden Scanapparatuur is HDD overwrite-erase vereist.
67.	Voor de door Inschrijver aangeboden Scanapparatuur is data sanitization vereist (= vernietiging achtergebleven data op HDD/SSD bij removal).
68.	Voor de door Inschrijver aangeboden Scanapparatuur is hergebruik van (onderdelen van) machines niet toegestaan.

1.10 Eisen ten aanzien van beveiligingscertificaten in het algemeen

Ten aanzien beveiligingscertificaten heeft de gemeente Amsterdam de volgende eisen:

Nr	Eisen ten aanzien van beveiligingscertificaten in het algemeen
69.	Inschrijver garandeert dat gebruikerstoegang tot de Scanvoorziening versleuteld plaats vindt.
70.	De door Inschrijver aangeboden Scanvoorziening maakt gebruik van SAN-certificaten, die per omgeving toegepast worden (Test, Acceptatie, Productie).
71.	In de door Inschrijver aangeboden Scanvoorziening zijn certificaten toegepast die Public Key Infrastructure Overheid (PKIO) of gelijkwaardig zijn.
72.	Inschrijver garandeert dat in de aangeboden Scanvoorziening geen Wildcard certificaten worden toegepast.

--EINDE--