Aanpassing van de Zoeksleutel encryptie

Samenvatting:

In OSO'18 willen we de huidige opzet met de zoeksleutel, een gecodeerde PGN, aanpassen, omdat:

- Huidige aanpak niet garandeert dat de PGN in de zoeksleutel ook de PGN is in de dossieraanvraag
- De zoeksleutel vaak niet correct gecodeerd blijkt of geen PGN blijkt te bevatten en dit pas (te) laat wordt gevonden. Hierdoor kan niet altijd teruggevonden worden waar een dossier is uitgewisseld en raakt de rapportage vervuild.

Hieronder worden drie alternatieven uitgewerkt; onze voorkeur gaat uit naar variant 3 omdat:

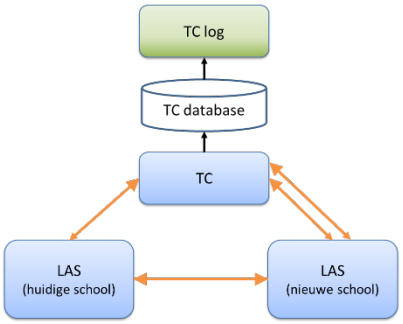
- Hierbij gegarandeerd is dat de overdracht plaats vind van een dossier met een PGN zoals ook door het TC wordt geregistreerd.
- Stoppen met het gebruik van de zoeksleutel die geen toegevoegde waarde heeft, nu we allen bewerker zijn.
- Het TC geen extra rekenwerk hoeft te verrichten bij het in- en uit- pakken van zoeksleutels tijdens de operatie.
- De benodigde aanpassingen in lijn zijn met het mogelijk overstappen op een later moment op een pseudo-id (ter vervanging van het PGN).

In het komende technische overleg zal een van deze drie alternatieven gekozen worden als aanpak in OSO'18.

Huidige versleuteling van zoeksleutel

In OSO wordt voor de 'normale' overdrachten een Dossier opgevraagd door de doelschool bij een bronschool op basis van de zoeksleutel. De zoeksleutel is dan het PGN; ofwel het BSN of wel het onderwijsnummer van de leerling waarover het dossier gaat. Omdat dit privacy gevoelige gegevens zijn, wordt de zoeksleutel geëncrypt bij het sturen van berichten naar het TC (en wordt het bericht verzonden over een beveiligd kanaal).

De huidige encryptie methode is gebaseerd op RSA en deze methode voldoet zonder meer aan de beveiligingseisen. Een kenmerk van deze methode is dat de resulterende versleutelde zoeksleutel bij eenzelfde waarde anders is bij iedere versleuteling.



In het TC worden binnengekomen berichten en verzonden antwoorden vastgelegd in een event tabel in de database. De TC log module verwerkt deze registraties periodiek en verstuurt ze naar de Kennisnet BI omgeving (zie figuur).

In de rapportage over OSO is het belangrijk om te kunnen tonen hoeveel unieke dossiers er zijn overgedragen. Doordat de RSA versleuteling leidt tot meerdere resultaten voor dezelfde PGN, wordt in de TC log module nu de zoeksleutel decrypt en vervolgens opnieuw versleuteld volgens een andere methode (die wel leidt tot eenzelfde resultaat bij eenzelfde input).

Dit leidt in de praktijk tot een aantal nadelen:

- In de TC log module moet de versleutelde zoeksleutel nu eerst gedecrypt worden en daarna opnieuw versleuteld. Dit is relatief duur en het originele PGN wordt 'zichtbaar'.

- Verkeerd versleutelde zoeksleutels kunnen niet gedecrypt worden en leiden tot ‘gaten’ in de rapportage.
- In de database van het TC is niet terug te vinden bij welke transacties één PGN betrokken is. Dit kan pas na de verdere verwerking in de BI omgeving (wat soms (te) laat is voor operationele ondersteuning).

Alternatieven

Om deze nadelen op te heffen, zijn er drie alternatieven op hoofdlijnen uitgewerkt. In de eerste variant wordt de zoeksleutel nog steeds toegepast, maar vinden er in het TC controles plaats op de inhoud van de zoeksleutel.

In de twee andere alternatieven verdwijnt de Zoeksleutel en wordt vervangen door de ‘pure’ PGN. Alle partijen binnen de OSO keten (inclusief Kennisnet) gelden juridisch als ‘bewerker’, wat betekent dat er geen noodzaak is om binnen de keten de PGN te versleutelen (ook omdat de communicatielijnen voldoende afgeschermd zijn).

In de eerste variant zonder zoeksleutel wordt een ‘simpele’ omzetting van alle OSO aanroepen beschreven, waarbij de zoeksleutel één-op-één vervangen wordt door de PGN.
Het derde alternatief maakt nog een extra stap: Hierbij wordt het TC ook het doorgeefluik van het PGN. In de aanroep van het doelsysteem naar het bronsystemen verdwijnen zowel de zoeksleutels als de PGN(!).

Alle alternatieven leiden tot aanpassingen voor zowel bron- en doel- systemen als het TC. Hieronder wordt per systeem aangegeven welke aanpassingen nodig zijn.

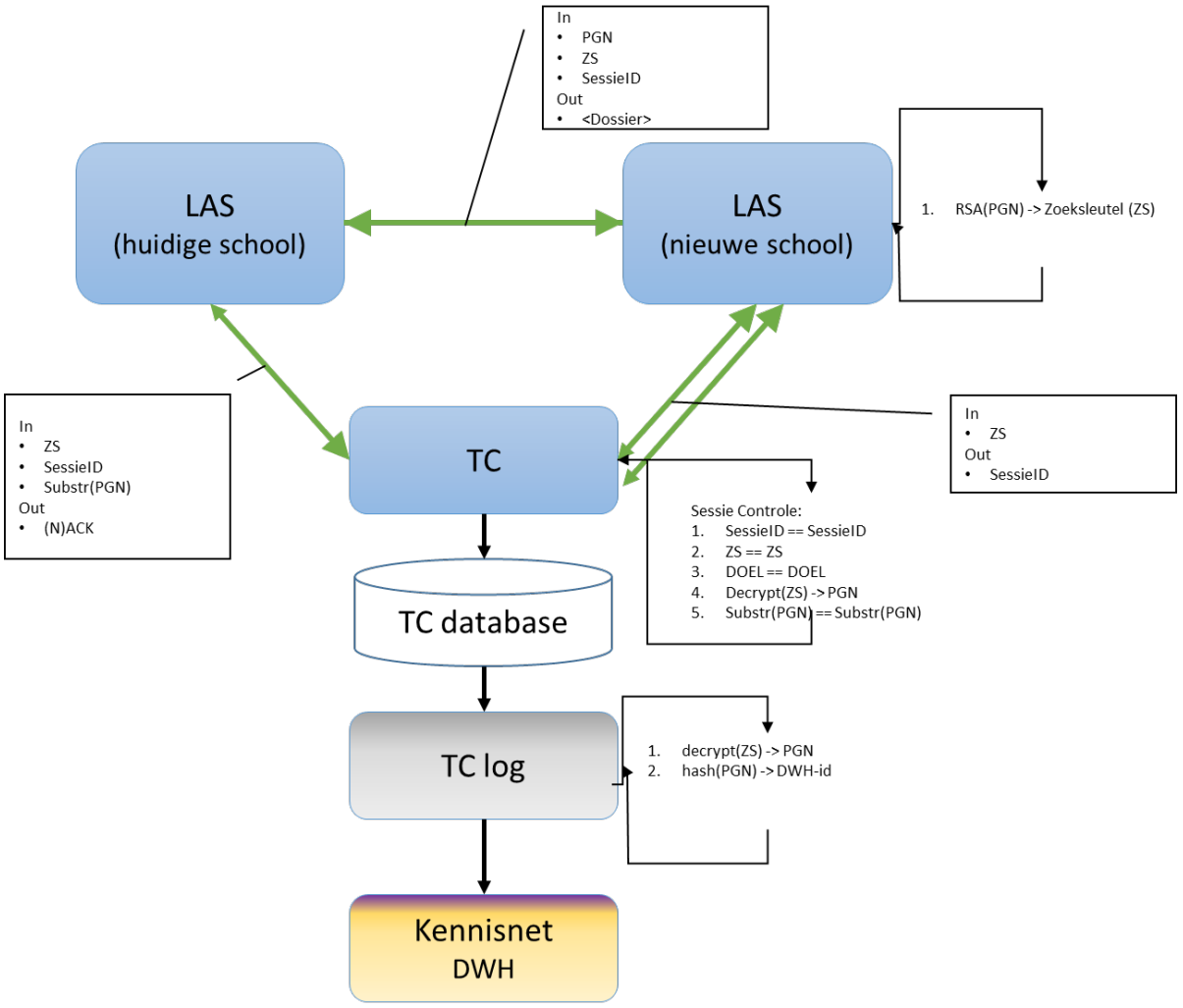
Criteria

Bij het zoeken naar en uitwerken van de alternatieven zijn de volgende criteria meegenomen:

1. Geen opslag ongecodeerde PGN
2. Vast kunnen leggen welk dossier is opgevraagd
3. Impact op keten
4. Duurzaamheid van oplossing

Het eerste criterium geeft aan dat bij het werken met ongecodeerde PGN’s in plaats van de zoeksleutel, er extra aandacht moet zijn om te voorkomen dat deze ook in die vorm vastgelegd worden in databases, log bestanden, etc.
Het tweede criterium betekent dat in het TC vast gelegd moet kunnen worden welk dossier er verstuurd is. (De huidige opzet voldoet niet aan dit criterium).
De derde afweging is om de impact op alle systemen in de keten te minimaliseren en zo gecontroleerd mogelijk te houden.
Bij het vierde punt wordt gekeken naar de houdbaarheid en robuustheid van de oplossing.

Voorstel 1: Controle op inhoud zoeksleutel door TC



In deze variant wordt bij het aanvragen van een sessie door het Doelsysteem, de zoeksleutel decrypt door het TC.; vervolgens wordt de PGN getest op correctheid. Als beide stappen slagen wordt een sessie toegekend. Het doelsysteem verstuurt vervolgens een dossier aanvraag aan het bronsysteem met daarin de sessie id, PGN en zoeksleutel (zoals nu ook het geval is). Bij het versturen van een sessie controle verzoek aan het TC stuurt het bronsysteem een sessie controle verzoek aan het TC met daarin de zoeksleutel, het sessie ID en de laatste vier karakters van het PGN.

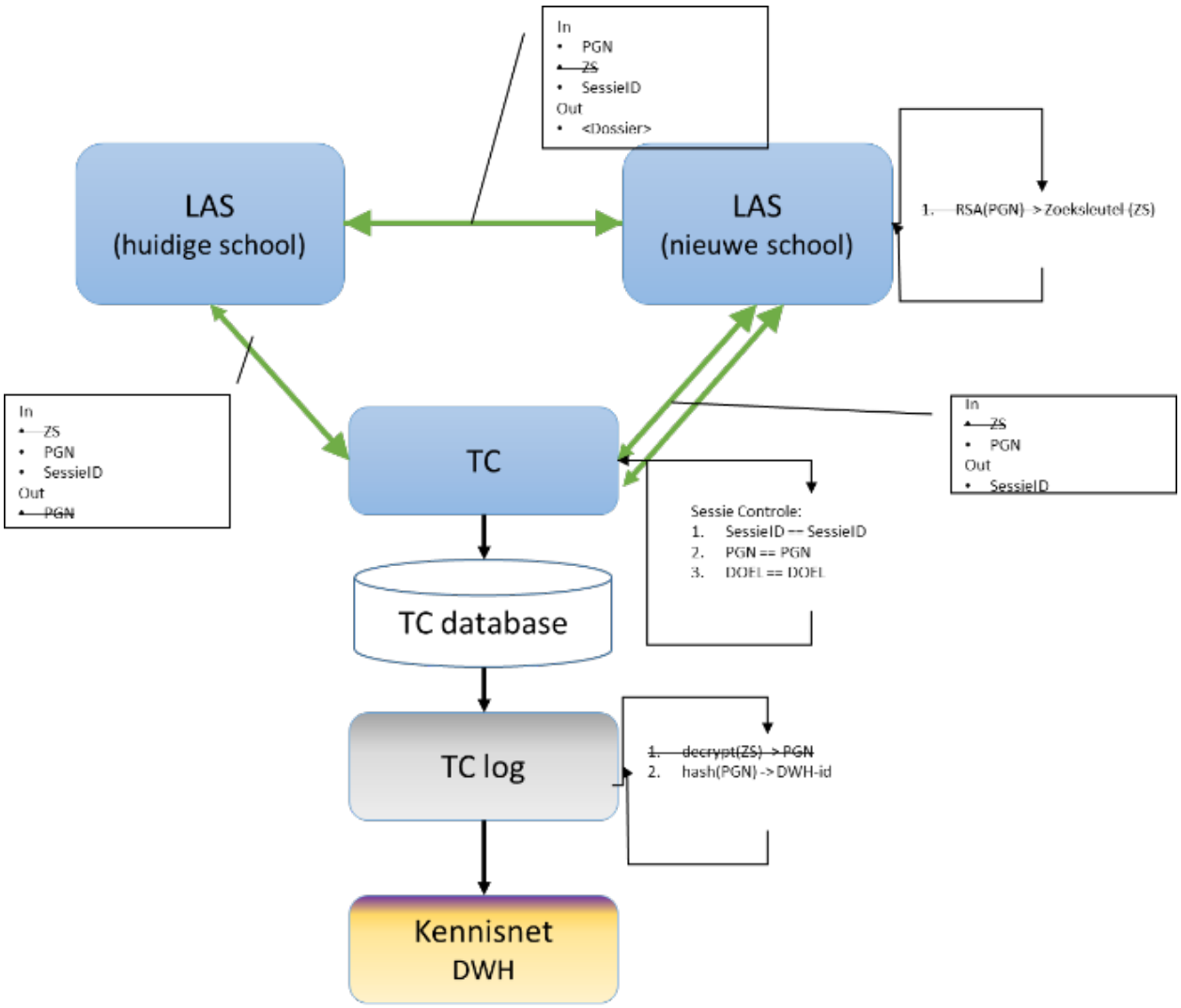
In het TC wordt dit stukje PGN vergeleken met hetzelfde deel van de uitgepakte PGN uit de zoeksleutel. Als deze overeenkomen wordt de sessie toegekend. Op deze wijze is het vrijwel zeker dat de opgevraagde PGN overeenkomt met die in de zoeksleutel én kan het TC die vastleggen.

Aanpassingen in Bronsystemen:
Bronsystemen moeten aan het sessie controle verzoek een deel van de ontvangen zoeksleutel meegeven. Er is geen nieuwe foutmelding nodig, ‘SessieAfwijkend’ zal door het TC worden terug gegeven wanneer de waarde van het controledeel van de PGN afwijkt (tov de zoeksleutel).

Aanpassingen in Doelsystemen:
Doelsystemen kunnen een nieuwe foutmelding ontvangen wanneer het TC bij het uitpakken en testen van de zoeksleutel een fout detecteert.

Aanpassingen in TC
In het TC moeten een aantal nieuwe controles en uitpak functionaliteit worden ingebouwd. De PGN moet 'vastgehouden' worden tussen het moment van sessie afgifte en weer opgeroepen kunnen worden bij sessie controle's. De sessie controle logica moet uitgebreid worden met de controle op de PGN.

Voorstel 2: PGN gebruiken ipv gecodeerde zoeksleutel



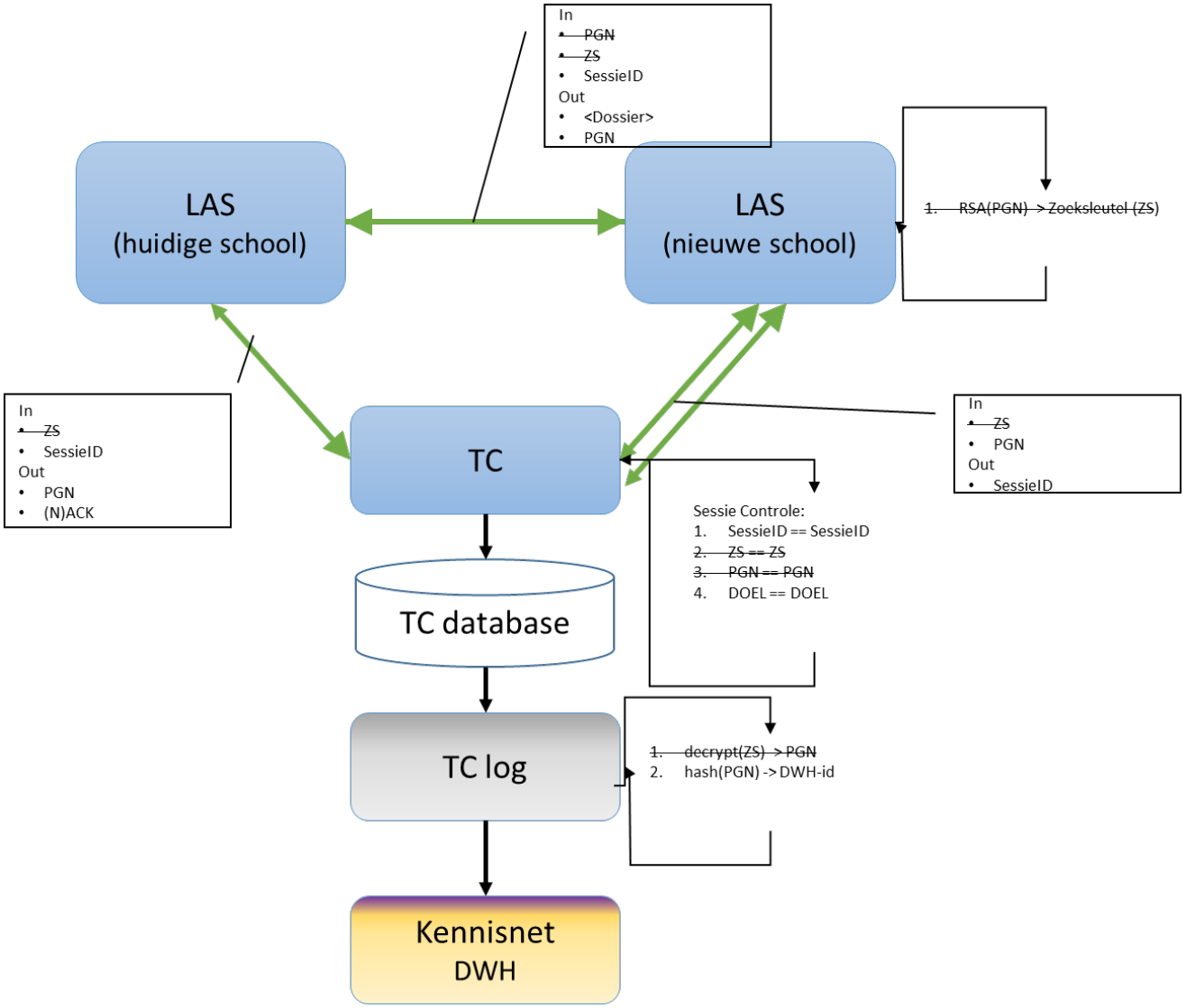
Aanpassingen in Bronsystemen:
Een bronsysteem krijgt niet langer een zoeksleutel in een aanvraag vanuit een doelsysteem (koppelsleutel blijft wel mogelijk).
Een bronsysteem moet in plaats van de zoeksleutel de PGN versturen naar het TC bij een sessie controle.
Er is geen nieuwe foutmelding nodig, 'SessieAfwijkend' zal door het TC worden terug gegeven wanneer de waarde van de PGN afwijkt (ipv de zoeksleutel).

Aanpassingen in Doelsystemen:
Een doelsysteem mag geen zoeksleutel meer maken, maar verstuurt in plaats daarvan bij zowel het aanvragen van een sessie (bij het TC) en het opvragen van een dossier (bij een Bronsysteem), de PGN.

Aanpassingen in TC
De aanroepen voor het aanvragen van een sessie en het controleren van een sessie worden aangepast; voortaan ontvangt het TC de PGN (en niet de Zoeksleutel). Bij een sessiecontrole wordt de PGN zoals het bronsysteem die ontvangt van het doelsysteem vergeleken met de PGN die het doelsysteem meegaf bij de sessie aanvraag.
Deze controle maakt de keten steviger, omdat de opzet met de zoeksleutel niet garandeerde dat de PGN die een doelsysteem opvroeg, gelijk was aan de PGN die gebruikt werd om de zoeksleutel te coderen.

In het TC moet de PGN gecodeerd opgeslagen, zowel in de database als in de logfiles. Hiervoor moeten zaken in het TC en de achterliggende systemen aangepast.

Voorstel 3: PGN gebruiken ipv gecodeerde zoeksleutel én doorgeven via TC



In deze variant wordt de PGN niet meer rechtstreeks meegegeven bij het aanvragen van een dossier door het Doel, maar wordt de PGN bij de sessie controle door het TC aan het bronsysteem gegeven. Op deze manier is uitgesloten dat een doelsysteem een ander dossier opvraagt dan bij het opvragen van een sessie.

Aanpassingen in alle systemen:
Omdat gewerkt wordt met ongecodeerde PGN's, moet ervoor gezorgd worden dat in logbestanden deze niet of alsnog gecodeerd wordt opgeslagen.

Aanpassingen in Bronsystemen:
Een bronsysteem krijgt alleen een sessieid mee bij een aanvraag vanuit een doelsysteem (koppelsleutel blijft wel mogelijk).
Een bronsysteem stuurt alleen de sessie id naar het TC bij een sessie controle.
Het bronsysteem krijg (wanneer de sessie controle positief is) van het TC de PGN terug die bij de sessie hoort. Pas daarna kan de verdere verwerking van het verzoek plaats vinden.
Er is geen nieuwe foutmelding nodig, 'SessieAfwijkend' zal door het TC worden terug gegeven wanneer de waarde van de PGN afwijkt (ipv de zoeksleutel).

Aanpassingen in Doelsystemen:
Een doelsysteem mag geen zoeksleutel meer maken, maar verstuurt in plaats daarvan bij het aanvragen van een sessie bij het TC. Bij het opvragen van een dossier (bij een Bronsysteem wordt alleen de sessie id meegegeven.

Aanpassingen in TC
De aanroepen voor het aanvragen van een sessie en het controleren van een sessie worden aangepast; voortaan ontvangt het TC de PGN (en niet de Zoeksleutel). Bij een sessiecontrole wordt de PGN doorgegeven aan het bronsysteem (als de sessie controle positief is.

Deze opzet maakt de keten steviger, omdat de PGN bij een sessie altijd via het TC wordt doorgegeven.

In het TC moet de PGN gecodeerd opgeslagen, zowel in de database als in de logfiles. Hiervoor moeten zaken in het TC en de achterliggende systemen aangepast.

Afwegingen en keuze

Alternatief	*Geen opslag ongecodeerde PGN*	*Vast kunnen leggen welk dossier is opgevraagd*	*Impact op keten*	*Duurzaamheid van oplossing*	*Opmerkingen*
Controle op inhoud zoeksleutel door TC	Voldoet	Voldoet (vrijwel zeker)	Relatief klein (maar vrij groot op TC)	Zoeksleutel blijft bestaan zonder echte functie, TC moet fors extra rekenwerk uitvoeren in operatie.	Gebruik zoeksleutel voegt geen extra veiligheid toe en kost in complexiteit en capaciteit
PGN gebruiken ipv gecodeerde zoeksleutel	Voldoet (met aanvullende maatregelen)	Voldoet	Aanzienlijk (verschuivingen in parameters aanroepen)	Zoeksleutel verdwijnt, ook stap richting toepassing pseudo-id	Overbodige PGN in aanvraag dossier blijft
PGN gebruiken ipv gecodeerde zoeksleutel én doorgeven via TC	Voldoet (met aanvullende maatregelen)	Voldoet (meer dan zeker)	Aanzienlijk (verschuivingen in parameters aanroepen)	Zoeksleutel verdwijnt, ook stap richting toepassing pseudo-id, overdracht gegarandeerd met vastgelegd PGN	Meest robuuste oplossing.