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. Het bronsysteem kan niet controleren of de zoeksleutel gecodeerd is met de PGN in het verzoek. In theorie kan een doelsysteem alle PGN's opvragen met één (bogus) Zoeksleutel.
- 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 wordt de op het Technisch Overleg gekozen variant 'Controle op inhoud zoeksleutel door TC' uitgewerkt. Deze aanpak heeft als belangrijke voordelen dat:

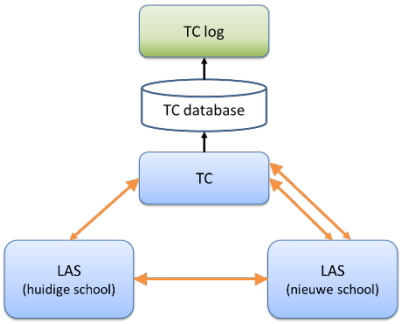
- Het 'PGN probleem' waarbij er geen relatie hoeft te zijn tussen Zoeksleutel en PGN in de document aanvraag wordt aangepakt.
- Foute zoeksleutels worden bij de Sessie aanvraag al gedetecteerd (en geven een nieuwe foutmelding op ipv een sessie).
- De impact voor aangesloten systemen laag is.

De beschreven wijzigingen zullen ook in het Programma van Eisen voor OSO'18 worden opgenomen.

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).

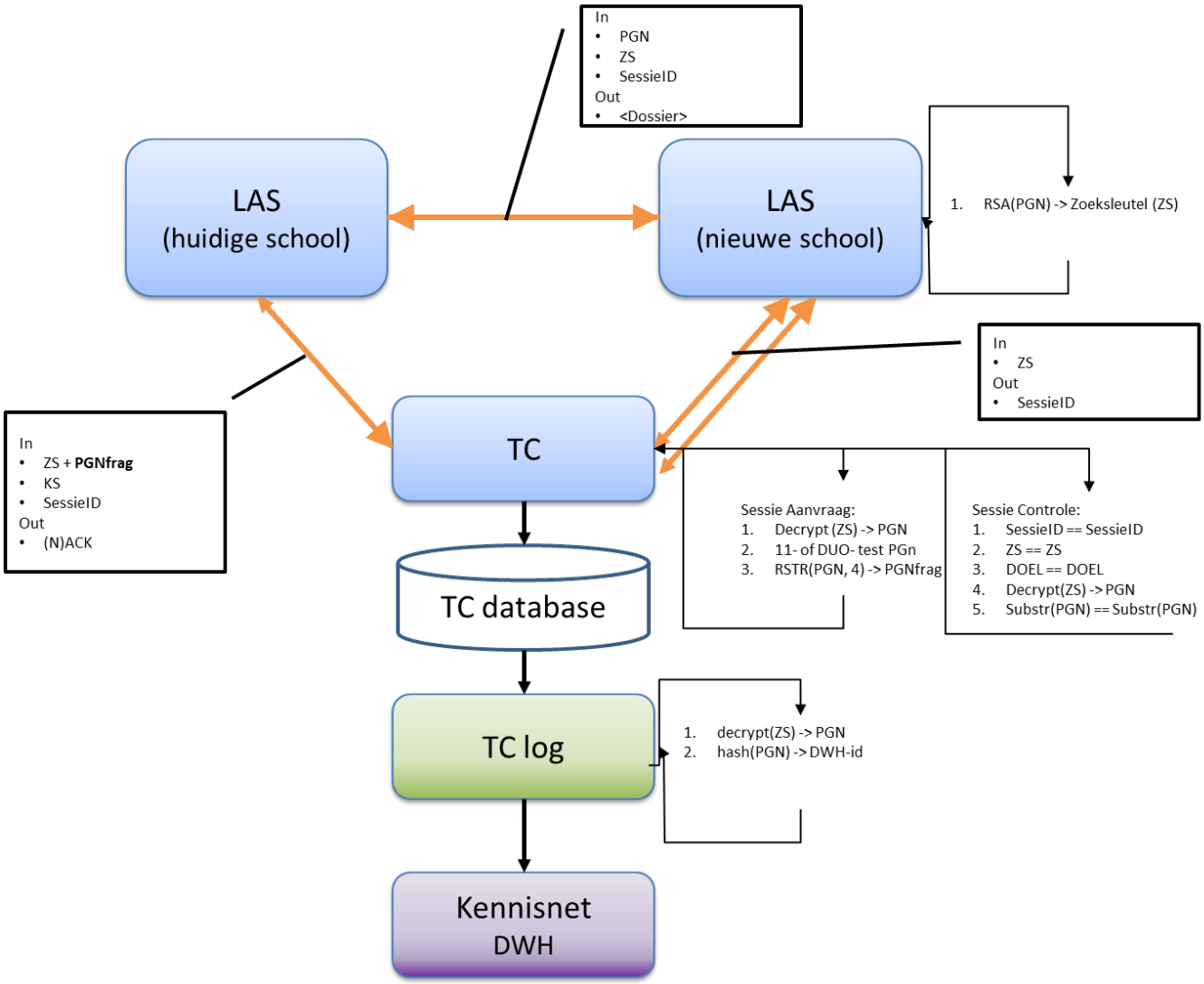
In de rapportage over OSO is het belangrijk om te kunnen tonen hoeveel unieke dossiers er zijn overgedragen. Doordat de RSA versleuteling leidt tot meerdere resultaten voor dezelfde PGN, wordt in de TC log module nu de zoeksleutel decrypt en vervolgens opnieuw versleuteld volgens een andere methode (die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

Aanpassing: Controle op inhoud zoeksleutel door TC

In de gekozen aanpak blijft de huidige werkwijze met Zoeksleutel toegepast worden. Het TC gaat wel de Zoeksleutel controleren op twee plaatsen in het proces:

- Bij het aanvragen van een Sessie wordt de Zoeksleutel gedecrypt. De PGN wordt gecontroleerd door het TC ('11 proef' voor BSN, 'DUO test' voor onderwijsnummer. Alleen als de PGN correct blijkt (en ook aan de andere voorwaarden is voldaan), wordt de sessie toegekend. Het TC slaat ook een deel van het PGN, het PGNfrag, op (het laatste/rechter vier karakters van PGN of Onderwijsnummer).
- Bij het controleren van de Sessie stuurt het bronsysteem de rechter vier karakters uit het ontvangen dossier verzoek mee naar het TC. In het TC worden deze vergeleken met die bij de Sessie opgeslagen PGNfrag. Als deze overeenkomen (en ook aan de overige eisen is voldaan) geeft het TC een positief resultaat terug.

Deze aanpak is in de onderstaande figuur weergegeven:



In deze aanpak 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 Doelsystemen: Extra foutmelding bij Sessie aanvraag
Doelsystemen kunnen een nieuwe foutmelding ontvangen wanneer het TC bij het uitpakken en testen van de zoeksleutel een fout detecteert. Deze foutmelding '**ZoeksleutelNietCorrect '** moet door Doelsystemen correct verwerkt worden.

Aanpassingen in Bronsystemen: PGNfrag bij Sessie controle
Bronsystemen moeten aan het sessie controle verzoek een de laatste/rechter vier karakters van de ontvangen zoeksleutel (BSN of onderwijsnummer) meegeven in de nieuwe parameter PGNfrag. Dit betekent dat de aanroep van de Sessie controle zal wijzigen en er een nieuwe parameter PGNfrag zal worden toegevoegd.

PGNfrag moet verplicht meegestuurd worden als er een Zoeksleutel wordt gebruikt bij het aanvragen van een Sessie ('normale' overstappen). Als er op basis van een Koppelsleutel wordt uitgewisseld (PaO) dan heeft het zenden van de PGNfrag geen zin (wordt door het TC genegeerd.)

Er is bij het controleren van een nieuwe sessie geen nieuwe foutmelding nodig; 'SessieAfwijkend' zal door het TC worden terug gegeven wanneer de waarde van de PGNfrag afwijkt van de bij de Sessie opgeslagen PGNfrag.

Geen aanpassingen in DocumentResponse
Er is geen extra foutmelding of parameter nodig in DocumentResponse. De huidige foutmelding, 'SessieAfwijkend', moet worden gebruikt als het TC constateert dat de sessie afwijkt (zie hierboven).

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 controles. De sessie controle logica moet uitgebreid worden met de controle op de PGN. Wanneer een fout in de Zoeksleutel geconstateerd wordt, moet dit door het TC geregistreerd worden in de event log tabel (via een nieuwe 'state') zodat deze ook in DWH rapportages zichtbaar worden.