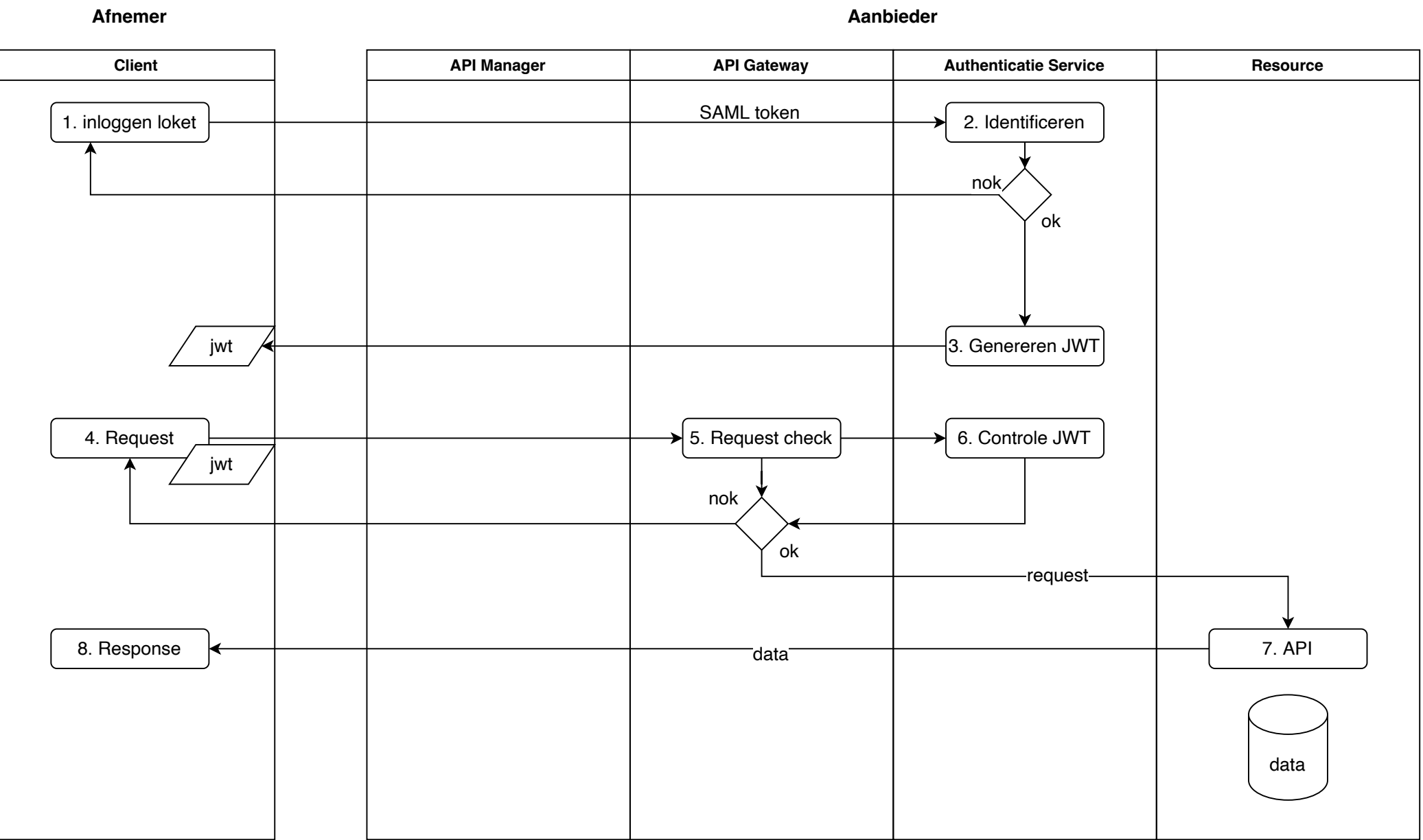


Casus Loket met SAML

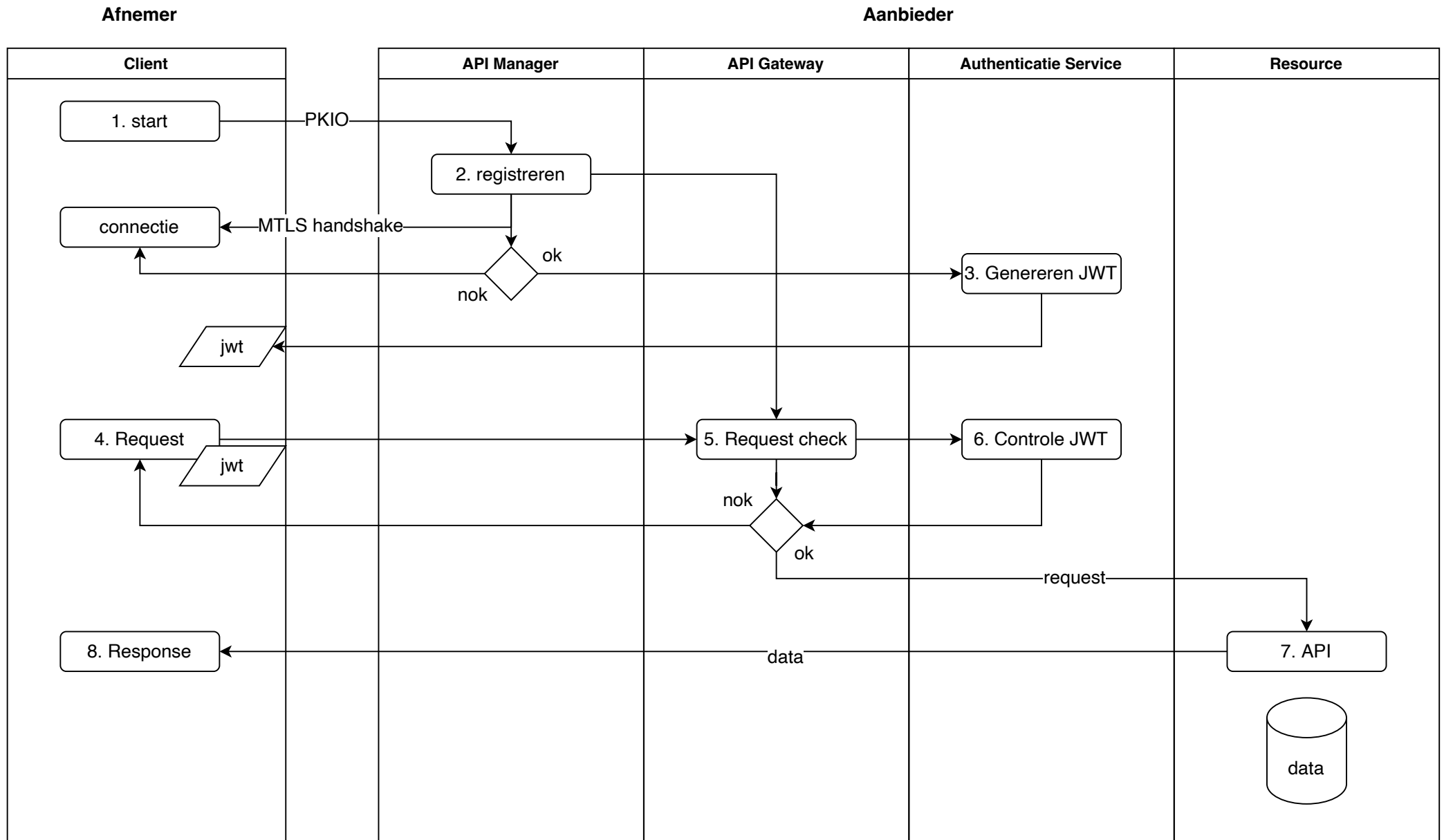


Casus API bevragen via loket en met client

Situatie Loket: Gebruikers die inloggen via het loket sturen een SAML token na inloggen aan de Authenticatie Service (1). De Authenticatie Service identificeert de gebruiker (2) op basis van het SAML token en stuurt een foutmelding terug naar het loket of genereert een jwt token (3) om terug te sturen.

Situatie Algemeen: Iedere API call moet zijn voorzien van een jwt (token) bij het request (4). De API Gateway verifieert of het request is voorzien van een token (5) en verifieert de geldigheid van het token bij de Authenticatie Service (6). Een request met een geldig token wordt doorgeleid naar de daadwerkelijke API upstream(7). Iedere uitzondering resulteert in een foutmelding terug naar de Afnemer. Indien alles goed is stuurt de API een response naar de afnemer met de data(8).

Casus Client met PKIO



Casus API bevragen via loket en met client

Situatie Client: De afnemer registreert z'n PKIO certificaat (met OIN) bij de API Manager(1&2). De Afnemer kan nu een MTLS connectie maken met de Aanbieder(3). De API Manager van de aanbieder verzoekt de Authenticatie Service om op basis van het OIN een jwt (token) te genereren en terug te sturen.

Situatie Algemeen: Iedere API call moet zijn voorzien van een jwt (token) bij het request (4). De API Gateway verifieert of het request is voorzien van een token (5) en verifieert de geldigheid van het token bij de Authenticatie Service (6). Een request met een geldig token wordt doorgeleid naar de daadwerkelijke API upstream(7). Iedere uitzondering resulteert in een foutmelding terug naar de Afnemer. Indien alles goed is stuurt de API een response naar de afnemer met de data(8).