

AUC9 Verstrekken sleutelmateriaal Dienstverleners

Het BSNk beheert en verstrekt via een Herkenningmakelaar cryptografisch sleutelmateriaal aan elke Dienstverlener (DV) die aantoonbaar beschikt over een PKIoverheid-certificaat. Indien de Dienstverlener geautoriseerd is om het BSN te verwerken verstrekt het BSNk speciaal BSN Sleutelmateriaal. De Dienstverlener ontsleutelt met dit Sleutelmateriaal het Versleutelde Identiteit of Versleutelde Pseudoniem van de Gebruiker dat de Dienstverlener verstrekt.

Voor eIDAS Outbound acteert de eIDAS Berichtenservice als Dienstverlener, die dienstbemiddelaar is voor de BRP. Daarom moet in deze use case het gebruik van de term "Dienstverlener", worden geïnterpreteerd als "Dienstaanbieder (hier: BRP) en/of eIDAS Berichtenservice (EB)".

Deze use case is een variant op de BSNk use case <AUC5>.

Stap	Actie	Omschrijving
	Initiële staat	Een Dienstverlener heeft Sleutelmateriaal nodig om de identiteit (bijv BSN) en/of pseudoniem uit de Versleutelde Identiteit/Pseudoniem te halen en vraagt zijn Herkenningmakelaar om hem hierbij te ondersteunen.
9.1	De Herkenningmakelaar valideert het verzoek.	De Herkenningmakelaar valideert dat het verzoek afkomstig is van bevoegd medewerker van de Dienstverlener, of een door deze geautoriseerde derde of zijn systeem.
9.2	De Herkenningmakelaar stuurt een aanvraag naar het Sleutelbeheer	De Herkenningmakelaar stuurt een aanvraag voor Sleutelmateriaal naar het BSNk Sleutelbeheer met daarin het PKIoverheid-certificaat van betreffende Dienstverlener.
9.3	Sleutelbeheer valideert de aanvraag	BSNk Sleutelbeheer controleert of de aanvraag daadwerkelijk en ongewijzigd van een erkende Herkenningmakelaar afkomstig is en of het meegeleverde PKIoverheid-certificaat van de Dienstverlener geldig is.
9.4	Sleutelbeheer controleert of Dienstverlener BSN mag ontvangen	BSNk Sleutelbeheer controleert of het OIN van de Dienstverlener zoals deze op het meegeleverde PKIoverheid-certificaat voorkomt op de Autorisatielijst BSN en ook Sleutelmateriaal mag ontvangen om een BSN te ontsleutelen.
9.5	Sleutelbeheer genereert Sleutelmateriaal	BSNk Sleutelbeheer genereert het Sleutelmateriaal voor het OIN van de Dienstverlener inclusief het BSN-Sleutelmateriaal indien diens OIN inderdaad voorkomt op de Autorisatielijst BSN
9.6	Sleutelbeheer versleutelt Sleutelmateriaal	BSNk Sleutelbeheer versleutelt Sleutelmateriaal obv de publieke sleutel op het meegeleverde PKIoverheid-certificaat van de Dienstverlener
9.7	Sleutelbeheer verstrekt Sleutelmateriaal aan de Herkenningmakelaar en registreert de verstrekking	BSNk Sleutelbeheer verstrekt Sleutelmateriaal ten behoeve van de Dienstverlener aan de aanvragende Herkenningmakelaar en registreert de verstrekking in een publiekelijk toegankelijke Sleutelverstrekkinglijst .
9.8	Herkenningmakelaar verstrekt Sleutelmateriaal aan de Dienstverlener	De Herkenningmakelaar verstrekt Sleutelmateriaal aan de betreffende Dienstverlener.
9.9	Dienstverlener ontsleutelt en installeert Sleutelmateriaal	De Dienstverlener ontsleutelt Sleutelmateriaal en installeert dit op zijn toegangssystemen.
	Finale staat	De Dienstverlener kan BSN en Pseudoniem uit een Versleutelde Identiteit/Pseudoniem halen. En de sleutelverstrekking is geregistreerd in het Sleutelverstrekkinglijst. De Dienstverlener kan via zijn HM diensten aansluiten en is klaar om gebruikers voor die dienst obv Persistent Pseudoniem of BSN te ontvangen.

NB: deze use case wordt gerealiseerd mbv [Interface specifications MR-BSNk](#)