

AAN Gebruikers van PKI certificaten

DATUM
REFERENTIE17 januari 2011
PON 11-004 Nieuwsbrief PKI 3**ONDERWERP** Resultaten enquête PKI en vervolgtraject**Vorbereidingen vervanging PKI-certificaten TenneT in 2011**

Om het berichtenverkeer tussen uw bedrijf en TenneT veilig te laten verlopen wordt de beveiligingstechnologie Public Key Infrastructure (PKI) gebruikt.

Op 6 september 2010 heeft TenneT u geïnformeerd over het project PKI. De geldigheid van de huidige PKI-certificaten verloopt op 5 oktober 2011. Het project PKI verzorgt de continuering van beveiligd berichtenverkeer ook na deze datum. TenneT dient alle deelnemers aan het berichtenverkeer een nieuw certificaat te verstrekken.

Op 14 december 2010 heeft TenneT u twee alternatieven voorgelegd met betrekking tot het moment van implementatie van certificaten met een hoger beveiligingsniveau. Middels een enquête bent u gevraagd de impact op uw IT systemen te bepalen en aan te geven of uw systemen hier tijdig gereed voor zullen zijn. Tevens hebt u kunnen aangeven wat uw *voorkeur* is met betrekking tot het moment van implementatie.

De resultaten van deze enquête zijn verzameld en hebben geleid tot een besluit over het vervolg van het PKI project. In deze nieuwsbrief wil TenneT u hierover informeren.

Alternatieven

TenneT heeft u in de vorige nieuwsbrief twee alternatieven voorgelegd:

1. Alternatief 1 betrof de implementatie van het hogere beveiligingsniveau vanaf 1 mei 2011;
2. Alternatief 2 betrof uitstel van het hogere beveiligingsniveau naar 1 april 2012. Dit heeft tot gevolg dat de periode tot 1 april 2012 overbrugd moet worden met tijdelijke certificaten van het huidige beveiligingsniveau.

Resultaten enquête

TenneT is verheugd met de grote hoeveelheid reacties op de enquête. Uw bijdrage om gezamenlijk tot de beste keuze te komen wordt zeer op prijs gesteld.

Op de vraag of marktpartijen klaar zullen (of kunnen) zijn voor het hogere beveiligingsniveau op 1 mei 2011 zijn de reacties gelijk (evenveel ja als nee). Gezien de grote respons betekent dit dat de helft van de marktpartijen dus niet op 1 mei 2011 klaar zullen of kunnen zijn, waarmee het risico op een niet succesvolle implementatie onverantwoord groot is.

Op de vraag welke voorkeur de marktpartijen hebben, is met ruime meerderheid voor uitstel van het hogere beveiligingsniveau gekozen. Als voornaamste reden is reductie van het risico genoemd.

Vervolg PKI-project

Op basis van de uitkomst van de enquête heeft TenneT besloten tot alternatief 2: uitstel. Alle deelnemers krijgen één jaar langer de tijd om de systemen gereed te maken voor het hogere beveiligingsniveau.

De verhoging van het beveiligingsniveau van de certificaten is essentieel om in de toekomst beveiligd berichtenverkeer te kunnen blijven garanderen. Gezien de onderlinge afhankelijkheid bij PKI (marktpartijen hebben hun eigen *private key* én elkaars *public key* nodig om succesvol berichten uit te wisselen) moeten alle marktpartijen tijdig in staat zijn het hogere beveiligingsniveau te ondersteunen.

Omdat de huidige certificaten verlopen op 5 oktober 2011, zullen in 2011 nieuwe certificaten van het huidige beveiligingsniveau uitgegeven worden met een geldigheid tot 1 oktober 2012.

In 2012 zullen opnieuw certificaten uitgegeven worden, ditmaal met het hogere beveiligingsniveau en een geldigheid tot 1 oktober 2016.

Planning situatie 2:

Jaar	2010		2011												2012													
	Maand	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
Inventarisatie marktpartijen		■																										
Keuze: eerst 1024 bits met SHA-1			■																									
Voorbereiding			■	■	■																							
Migratie						■	■	■	■	■	■	■																
Impactanalyse 2048 bits met SHA-2			■	■	■	■	■	■	■	■	■	■																
Voorbereiding													■	■	■	■	■	■										
Migratie																			■	■	■	■	■	■	■	■	■	

Gevolgen voor de marktpartijen

Samenwerking Diginotar

TenneT draagt momenteel zelf zorg voor de beveiliging van het Edine berichtenverkeer over het CPS middels de uitgifte van PKI-certificaten. TenneT heeft onderzoek gedaan om dit uit te besteden, hiermee beoogt TenneT een nog hoger kwaliteitsniveau van de dienstverlening. Dit heeft geleid tot samenwerking met Diginotar.

Diginotar is TTP (Trusted Third Party) en staat als "Aanbieder van gekwalificeerde certificaten" geregistreerd bij de OPTA. Diginotar is onderdeel van VASCO. U zult al bij de eerstvolgende migratie uw certificaat van Diginotar ontvangen en niet meer van TenneT.

Voorbereiding en migratie 2011

Om ook in de toekomst beveiligd berichtenverkeer te kunnen garanderen, dient u rekening te houden met de vervanging van de huidige certificaten door nieuwe certificaten van het huidige beveiligingsniveau. Evenals in voorgaande projecten zal deze vervanging gefaseerd uitgevoerd worden. TenneT werkt momenteel het migratieplan uit, u ontvangt zo spoedig mogelijk meer informatie.

Hoewel de certificaten technisch hetzelfde zijn, is goede voorbereiding onontbeerlijk. Denkt u hierbij aan het reserveren van resources, het informeren van uw leveranciers en het opfrissen van kennis en documentatie.

Impactanalyse, voorbereiding en migratie 2012

U heeft tot 1 april 2012 om uw systemen gereed te maken voor de nieuwe certificaten met het hogere beveiligingsniveau (RSA 2048 bits sleutellengte met SHA-2 hash algoritme). U kunt hier nu al uw voorbereidingen voor treffen, zoals een impactanalyse op uw systemen. Nadat alle marktpartijen het nieuwe SHA-1 certificaat in gebruik hebben genomen, zal TenneT de marktpartijen actief begeleiden bij de voorbereidingen. Er zal onder andere een testomgeving beschikbaar gesteld worden.

Middels deze brief vertrouwt TenneT erop u meer inzicht gegeven te hebben in de komende werkzaamheden rondom PKI. U ontvangt zo spoedig mogelijk meer informatie over de migratie, zoals de planning, procedures etc.

Voor vragen kunt u contact opnemen met de projectleider de heer J. Stikvoort via telefoonnummer +31 (0)26 373 3168 of via e-mailadres pki-cps@tennet.eu.

U kunt deze informatie ook vinden op onze website www.tennet.eu > Klanten > Diensten.