

TO Users of PKI certificates

DATE

17 January 2011

REFERENCE

PON 11-004 Newsletter PKI 3

ITEM Results of PKI survey and process continuation

Preparations for replacing PKI certificates at TenneT in 2011

We use Public Key Infrastructure (PKI) security technology to safeguard communication between your company and TenneT.

On 6 September 2010, TenneT informed you about its PKI project. The existing PKI certificates expire on 5 October 2011. The PKI project will continue to assure secure communication beyond that date. TenneT must issue a new certificate to all communication participants.

On 14 December 2010, TenneT presented two alternatives to you with regard to the moment of implementation of higher-security certificates. By means of a survey you were asked to determine the impact on your IT systems and to indicate whether your systems will be ready for this process on time. You were also able to indicate your *preference* for the moment of implementation.

The results of the survey have been collected and have led to a decision on the continuation of the PKI project. The present newsletter is intended to inform you about this.

Alternatives

In the previous newsletter TenneT proposed two alternatives:

1. Situation 1 concerned the implementation of the higher security level as of 1 May 2011.
2. Situation 2 concerned the postponement of the implementation of the higher security level to 1 April 2012. If this alternative is opted for, temporary certificates of the present security level will need to be used during the period up to 1 April 2012.

Survey results

TenneT was pleased with the large number of completed surveys received. We really appreciate your contribution, which has enabled us to select the best option.

The reactions to the question whether market parties will (or can) be ready for the higher security level on 1 May 2011 were split equally (yes as often as no). In view of the great number of reactions, this means that half of the market parties will not or cannot be ready on 1 May 2011, so that the risk of unsuccessful implementation is so considerable that it would be irresponsible to opt for this alternative.

When asked for their preference, the vast majority of parties opted for postponement of the implementation of the higher security level. The main reason stated was risk reduction.

Continuation of the PKI project

Based on the outcome of the survey, TenneT has decided to go for Situation 2: postponement. All participants will have an extra year to prepare their systems for the higher security level.

The increase in the security level of the certificates is essential for us to be able to keep guaranteeing secure message traffic in the future. In view of the interdependence with PKI (market parties need their own *private key* as well as each other's *public key* to be able to successfully exchange messages), all market parties must be able to support the higher security level in a timely manner.

The existing certificates expire on 5 October 2011, so it will be necessary to issue new certificates in 2011 for the present level of security. These certificates will be valid until 1 October 2012. Certificates will be reissued in 2012 for the higher security level and will be valid until 1 October 2016.

Planning for Situation 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																												

Consequences for market parties

Collaboration with Diginotar

At the moment, TenneT itself secures the Edine message traffic across the CPS by issuing PKI certificates. TenneT has investigated the possibility of outsourcing this task to realise a higher level of service quality. This resulted in our collaboration with Diginotar.

Diginotar is a TTP (Trusted Third Party) and is registered with OPTA as a "Provider of qualified certificates". Diginotar is a subdivision of VASCO. When the next migration takes place you will already receive your certificate from Diginotar rather than TenneT.

Preparation and migration in 2011

To be able to keep guaranteeing secure message traffic in the future, we will need to replace the current certificates with new certificates of the present security level. Please be aware of this. As in previous projects, the replacement will take place in stages. TenneT is currently drawing up the migration plan and you will receive more information as soon as possible.

Although the certificates are technically the same, thorough preparation will be vital. Think of reserving resources, informing your suppliers and refreshing your knowledge and documentation.

Impact analysis, preparation and migration in 2012

You will have until 1 April 2012 to prepare your systems for the new certificates with the higher security level (RSA 2048 bits key length with SHA-2 hash algorithm). You can already start making preparations, like the performance of an impact analysis on your systems. Once all market parties have started using the new SHA-1 certificate, TenneT will actively guide them through their preparations. Among other things, a test environment will be made available.

We trust that this letter has provided you with a better understanding of TenneT's planned activities relating to the PKI certificates. You will receive more information on the migration, such as planning, procedures, etc., as soon as possible.

If you have any questions, you can contact the project leader, Mr J. Stikvoort, via telephone number +31 (0)26 373 3168 or by e-mail at pki-cps@tennet.eu.

You can also find this information on our website at www.tennet.eu > Customers > Services.