Qualified Electronic Signature (QES) x Nect Sign

In today's Expert Talk, our two Senior Sales Managers Eike Müller and Ingmar Besch, who joined our team last year, answer our questions on the subject of Qualified Electronic Signature (QES).

Both of them can draw on many years of professional experience and have had formative stations in their careers. Eike has worked for Telefonica Germany in wholesale and partner business as well as business development roles and market development from the Identity Verification as a Sercive sector. Ingmar has held and taken on various sales, key account management and business development roles in his career at trust centers, banking and industry. Together, the two bring the knowledge and strength that the Nect team needs to establish itself with QES.

But what exactly is meant by a qualified electronic signature?

QES is regulated throughout the EU by the eIDAS Regulation and places high demands on the identification of the signatory and the creation of signatures. Certification and monitoring by the BNetzA (Federal Network Agency) is required for the creation of signatures (as a so-called trust center or qTSP - qualified trust service provider). This involves both technical requirements (such as dedicated and certified signature creation units in HSMs - high-security modules), but also procedural and organizational requirements (e.g., physical security of data centers or designation of responsible employees).
The identification of signers must have at least the security level „substantial" or „high" according to eIDAS Regulation §24. This also requires certification by the BNetzA with fulfillment of supplementary requirements by the BSI. Nect achieved this certification in the summer of 2021.

What types of digital signatures are there?

There are three different types:

- **the simple electronic signature (EES).**
- **the advanced electronic signature (FES).**

the qualified electronic signature (QES).

Under a simple electronic signature (EES), identification does not have to be taken into account, nor does a recognizable change to the document. The data used is data that is attached in electronic form to other electronic data. This data is then used in a further step for signing. Since this form of signature is very easy and quick to perform, it is, however, more difficult to prove than the FES and QES, since the EES cannot be clearly assigned to a person.

With the advanced electronic signature (FES), the identification of the signer is made possible and thus clearly assigned to the person. The signature is created using electronic signature creation data, which the user (signer) can use with a high degree of self-confidence. It is linked to the data signed in this way in such a way that any subsequent change to the data can be detected.

With the qualified electronic signature (QES), the first step is to verify the identity of the person before signing.

In the next step, a certified trust center issues an electronic certificate bearing the name of the signatory. This then enables the user to trigger qualified signatures (once or several times, depending on the type of certificate). This form of signature uses configured software or hardware to create a signature. A QES is used with an electronic certificate issued by an accredited trust service provider. A key characteristic of a qualified certificate is that the identity of the signer is immediately recognizable when the document is opened. This is ensured by extensive requirements for a qualified certificate.

Why is eIDAS certification an important requirement?

The eIDAS certification ensures the high standard required of those responsible and involved. This proof must be confirmed at regular intervals by surveillance audits or re-certifications. This ensures a high level of security for the user of a QES, because a QES must still be verifiable in 10, 20 or 30 years.
Nect has been an eIDAS certified company since last year, which fulfills the legal framework and therefore Nect Ident can be used to trigger a QES.

Why is a trust service provider needed as a partner for issuing the QES?

Electronic certificates for QES may only be issued by certified and approved trust centers. These are regulated throughout the EU and are listed centrally here: Link
Nect cooperates with the German trust service provider Bank-Verlag GmbH, which offers a flexible solution for integrating qualified and advanced signatures into its own products. Thus, a signature is possible directly in the Nect Wallet, which enables a continued excellent customer experience and conversion rate of our solution.

Due to an approval of the Trust Center by the German Federal Network Agency, our solution is totally made in Germany.

What happens technically during a QES?

The user is identified by means of Nect Ident. The data is transmitted to the Trust Center for the issuance of an electronic certificate. There, the QES is calculated in a signature creation unit using extensive cryptographic processes. This electronic certificate is inserted into an electronic document (preferably pdf.). With it then in the Adobe Acrobat reader e.g. the green hook is indicated. If you go to the signature field, the certificate details are displayed until issued by the Trust Center.

What does the process look like for the user?

For the user, the process is designed with maximum simplicity and convenience. To successfully identify themselves, the user goes through two steps. First, a video recording of the ID document is required, as well as a selfie video of the user. Before signing, the document is checked and approved by a TAN via cell phone number and then successfully signed with a QES. The process takes less than 2 minutes.

What sets Nect apart from other providers?

Nect was the first company to establish a fully digital process. With Nect Ident, users identify themselves fully automatically, without waiting, no matter when, no matter where, and with a high success rate. Semi-digital processes such as a video ident or analog processes such as post ident are now a thing of the past. So the user can experience a positive and efficient user experience, through a fully digital process. Integration into the existing user flow requires little IT effort.