

Requirements imposed by the
Electronic Record Procedure
(eANV) on the software used

Consist ITU
Environmental Software GmbH
02.03.2009

To implement the specifications of the Electronic Record Procedure, besides a series of functional requirements, additional requirements must be met which result from the use of qualified electronic signatures.

The following list summarizes the most important requirements. It should particularly be noted that the Digital Signature Act prescribes a manufacturer declaration for the signature application component used, or a confirmation by the Federal Network Agency (BNetzA) based on certification according to Common Criteria (CC) at a security level of at least EAL 3+.

1 Requirements imposed by the Ordinance on Waste Recovery and Disposal Records (NachwV)

The NachwV specifies that for certain disposal processes, only electronic documentation will be used in the future. The required contents are prescribed by the NachwV, while the format of the documents is specified by the BMU interface (currently in version 1.04). These are complex XML documents which contain surrounding electronic signatures for parts of the documents as specified by XMLDSIG, or more specifically by the XAdES-T standard.

The documents are electronically transmitted between participating organizations, with all communication with the central system of the agency (ZKS) requiring the OSCI protocol.

Electronic signatures must moreover be implemented as qualified electronic signatures (QES) in accordance with the Digital Signature Act (SigG).

Another requirement is the maintenance of an electronic register, which requires storage for many years.

2 Requirements imposed by SigG

To create QES, secure signature generation units with qualified certificates are needed, that is, signature cards and card terminals (with approval of the Federal Network Agency) and a suitable signature application component (SAK).

The manufacturer declaration is issued in accordance with the guidelines of the BNetzA. The manufacturer declares conformity with SigG and provides additional documentation supporting that conformity and security, including appropriate test results, documentation of functionality, and the requirements for the implementation environment. After successful approval, the BNetzA publishes the manufacturer declaration. A manufacturer declaration is already stored by the BNetzA upon submission, and so the SAK can then already be used for QES.

The approval of an SAK is granted by the BNetzA based on a CC certification of a security level of at least EAL 3+ (SigV, Annex 1). Certification is granted based on general security requirements for the security level, which are specified in a specific requirements catalog (Protection Profile) for the concrete application. There is currently no uniform Protection Profile for SAKs. So right now, the individually created Protection Profiles of the various SAK manufacturers are used.

The approval procedure is very costly and, particularly for higher Protection Profiles, oriented towards specific application scenarios, such as security environments in the military arena. Particularly for commercial applications, such as for registration of the deduction of input tax in electronic invoicing, the SigG thus explicitly provides for manufacturer declarations as an alternative.

3 Satisfying requirements with MODAWI

Modawi can handle the creation, modification, storage, and communication of electronic messages. For signature generation and verification, SecCommerce products provide a SigG-compliant security component. In addition, the MO-DAWI-SAK solution also covers multiple signatures, batch signatures, and signature archival. For practical use, the MODAWI solution supports a wide variety of system architectures.

Modawi's security application component has a manufacturer declaration, and thus is entirely compliant with legal requirements. The SecCommerce products are currently in the process of certification according to Common Criteria EAL 3+ for SigG approval by the Federal Network Agency, which will represent an additional proof of security, enabling its use in even more demanding environments.