

How to sign an XML JPK file using proCertum SmartSign for submission to the Tax Office

Igor Kyrzewski · 26.01.2026 · Ogólne

The Uniform Control File (JPK) is a standard XML file format in which taxpayers submit accounting and tax data to the Ministry of Finance. In some cases (e.g., JPK upon request from the office, older versions, or specific structures), it is required to sign the file with a qualified electronic signature before sending. Certum is one of the trusted providers of qualified certificates in Poland, and the program **proCertum SmartSign** allows for the convenient signing of XML files in the required XAdES format.

The following instruction describes the step-by-step process of configuring and signing a JPK file, based on the manufacturer's (Certum) recommendations and the guidelines of the Ministry of Finance.

Prerequisites

- A valid qualified electronic certificate issued by Certum (on a cryptographic card, USB token, or in the SimplySign cloud).
- A cryptographic card reader (if you are using a card).
- The installed **proCertum SmartSign** program – download the latest version from certum.pl or pomoc.certum.pl.
- A JPK file prepared in XML format (generated from accounting software or the Ministry of Finance application).

Step 1: Configure signature settings in proCertum SmartSign

Before the first signing of the JPK file, configure the program so that the signature complies with the requirements of the Ministry of Finance (XAdES internal/enveloped format).

1. Launch the **proCertum SmartSign** program.

2. Go to the **Settings** menu → **Signature** section.
3. Set the following parameters:
 - **Signature format**: XAdES
 - **Signature type**: Internal signature
 - **Hash function**: SHA-256
 - **Signature variant**: Do not include additional information (BES)
4. **Advanced XAdES signature options**:
 - Select: **Create an enveloped signature** when signing the XML document with an internal XAdES signature
 - Select: **Create a signature for JPK** (this option is crucial for JPK files)
 - Optionally: Check **Check certificate validity online before starting signing**.

These settings ensure that the signature will be internal (enveloped), and the signed file will retain the .xml extension and will be accepted by the Ministry of Finance systems.

Step 2: Sign the JPK XML file

1. In the proCertum SmartSign program, go to the **Signing** tab.
2. Click the **Add file** button and select the prepared JPK file in .xml format.
3. The file will appear in the list. Click the **Sign** button (or **Sign all** if there are multiple files).
4. Select the appropriate qualified certificate (it should be visible after inserting the card/token or activating it in the cloud).
5. Enter the certificate PIN.
6. Confirm the operation. The program will create a signed file (usually with the same .xml or .xades extension – depending on the context).

After signing, check the status in the program – it should display information about the successful submission of the qualified signature.

Step 3: Verify the signature (optional)

Before sending, it is worth verifying the signature:

- In proCertum SmartSign, go to the **Verification** tab.
- Add the signed file and check the result.

You can also use the online tools of the Ministry of Finance or the Certum website for verification.

Common issues and notes

- If the signature fails validation: check if the option "Create a signature for JPK" and enveloped are selected.
- The qualified signature must be issued to a person authorized to represent the taxpayer.
- For JPK_V7M/K, it is often sufficient to sign with the authorizing data (revenue amount from the previous declaration) – qualified signature is optional or required only in specific situations.
- Update the SmartSign program to the latest version to avoid compatibility issues.

By following these steps, the JPK file will be correctly signed and ready for secure submission. If in doubt, use the technical support of Certum or the helpline of the Ministry of Finance. Good luck!