



UWP



Digital signatures



WINDOWS > GUIDES > SIGNATURES > DIGITAL SIGNATURES

Explore digital signatures for Windows security

Nutrient supports the following signing methods:

- ✦ **PAdES** (PDF Advanced Electronic Signatures, ETSI.CAdES.detached)
- ✦ **CMS** (adbe.pkcs7.detached)

Supported signing algorithms are:

- ✦ **RSA**
- ✦ **ECDSA**

Supported hashing algorithms include:

- ✦ **MD4**
- ✦ **MD5**
- ✦ **SHA-2** (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512-256)

A hashing algorithm is an algorithm that converts a large amount of data (your PDF document) to a fixed-length string. If someone changes one bit of data in your PDF document, the hashing algorithm produces a different string, so if you store that hash inside the PDF document, you could potentially know when it has been changed by a third party. However, as easy as it sounds, this approach is insecure. If someone knows the hashing algorithm that was used to sign the PDF, they could replace the hash inside the PDF so that it validates as authentic. To avoid this, Nutrient works with encryption algorithms.



ASK AI

More specifically, Nutrient supports `RSA`, one of the most popular public key encryption algorithms. `ECDSA`, an algorithm based on elliptic curve cryptography, is also supported. Cryptographic systems based on `ECDSA` are becoming the de facto standard for messaging and systems security.

Was this helpful?

☒ YES

☐ NO

Questions? [Contact us](#)

