1 Introduction

This document describes the TU Services feature for building a PDF Advanced Electronic Signature (PAdES), from a valid NemID signature (NemID XMLDSig).

2 PAdES

A PAdES document, is a signed PDF which conforms to the PAdES specification and is used both as a long-term storage container for the contained sigantures and as an visually easy to verify by the end-user digital signature.

Refer to the description of how TU Services creates the PAdES and to the examples available on https://authentication.signaturgruppen.dk

3 PAdES and NemID

A NemID XMLDSig is a digital signature within a envelope style XML document, conforming to the XMLDSig standard for digital signatures.

The XML document is a valid digital signature on its own, but is is not easily verified or viewed by end-users. It requires specialized software and expert knowledge to verify and extract the information from the XMLDSig document.

TU Services features a specialized API, using the SPS.Client library, which constructs a PAdES document from a valid NemID XMLDSig document.

The resuling document is visible verifiable in any Adobe Reader (version 10+) and contains both the signed document, the NemID XMLDSig and all relevant information needed in order to verify the signature in a court of law. Furthermore, the PAdES is Long Term Validation (LTV) enabled, which means that all required revocation list information is included in the PAdES document and that the document is signed both by a valid and Adobe approved hardware-backed signing key and is signed by an external timestamp service.

This makes the PAdES the optimal container for both long-term storage of the NemID signature as well as the only was to produce a NemID signature, that anyone can see and verify.

4 Building a PAdES document

In order to construct the PAdES from a NemID XMLDsig you first need the required feature in TU Services (contanct Signaturgruppen for that one), and then you use our API by calling:

```
var padesBytes = new AdvancedElectronicSignaturesService().CreatePades(xmldsigBytes);
```

5 Setting up trust for TEST PAdES

If you test the integration in our TEST environment, the returned PAdES is signed by our TEST signing certificate.

In order to verify this signature in Adobe Reader, do the following in Adbobe Reader:

1: Edit- > Settings- > Signatures- > Verification

2: Under Windows Integration- > check both checkmarks

3: Import the following certificate into "Trusted Root Certification Authorities". This can be done by clicking the .cer file in Windows or by using MMC.exe - > add/remove snap-in- > certificates- > local machine - > select "Trusted Root Certification Authorities"- > import- > Accept dialog

```
https://www.signaturgruppen.dk/download/platformspakke/SPS.Client/docs/SignaturgruppenPDFSigningCaTest.p12.cer
```

4: Restart Adobe Reader and open the TEST PAdES.

NOTE: In our TEST environment, only NemID XMLDSigs created in the NemID TEST environment are accepted.

6 Contact information

Info	
Mail	support@signaturgruppen.dk
Phone	+45 70256425
Website	https://www.signaturgruppen.dk