

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastuktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

## Änderungsbedarf in gemSpec\_Kon

### TIP1-A\_5447 - Einsatzbereich der Signaturvarianten

Der Signaturdienst MUSS für die Erstellung und Prüfung von nicht-qualifizierten elektronischen Signaturen (nonQES) und qualifizierten elektronischen Signaturen (QES) die Vorgaben zum Einsatzbereich gemäß Tabelle TAB\_KON\_778 umsetzen.  
[<=]

**Tabelle 1: TAB\_KON\_778 – Einsatzbereich der Signaturvarianten für XAdES, CAdES und PAdES**

| Signaturvarianten |                  |  |   | Einsatzbereich |                         |                             |
|-------------------|------------------|--|---|----------------|-------------------------|-----------------------------|
| Signaturverfahren | Signaturvariante | WAS wird signiert?   | WO wird die Signatur abgelegt?              | nonQES         | QES Außen-schnittstelle | QES Fachmodul-schnittstelle |
| XAdES             | detached         | beliebiges (Binär)-Dokument  | außerhalb des Dokuments in der SignResponse | Nein           | Nein                    | Nein                        |
| XAdES             | detached         | gesamtes Input XML-Dokument (= Root-Element mit Subelementen)          | außerhalb des Dokuments in der SignResponse | Nein           | Nein                    | Nein                        |
| XAdES             | detached         | ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument | außerhalb des Dokuments in der SignResponse | Nein           | Nein                    | Nein                        |

|       |            |  |   |      |               |               |
|-------|------------|--|---|------|---------------|---------------|
| XAdES | detached   | ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument | Innerhalb des Dokuments, aber außerhalb des signierten Subbaums | Ja   | Bedingt       | Ja<br>Bedingt |
| XAdES | enveloped  | gesamtes Input XML-Dokument (= Root-Element mit Subelementen)          | Als direktes Child des Root-Elements                            | Ja   | Ja<br>Bedingt | Ja<br>Bedingt |
| XAdES | enveloped  | ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument | Als direktes Child des ausgewählten Elements                    | Ja   | Nein          | Ja<br>Bedingt |
| XAdES | enveloping | gesamtes Input XML-Dokument (= Root-Element mit Subelementen)          | Im Dokument, das Root-Element umschließend                      | Ja   | Ja<br>Bedingt | Ja<br>Bedingt |
| XAdES | enveloping | ausgewähltes nicht Root-Element mit Subelementen im Input XML-Dokument | Im Dokument, das ausgewählte Element umschließend               | Nein | Nein          | Nein          |
| CAdES | detached   | gesamtes Binärdokument   | außerhalb des Dokuments in der SignResponse                     | Ja   | Ja            | Ja            |
| CAdES | enveloping | gesamtes Binär-Dokument  | innerhalb des CMS-Dokuments                                     | Ja   | Ja            | Ja            |

|       |   |                              |                     |    |    |    |
|-------|---|------------------------------|---------------------|----|----|----|
| PAdES | - | gesamtes<br>PDF-<br>Dokument | Im PDF-<br>Dokument | Ja | Ja | Ja |
|-------|---|------------------------------|---------------------|----|----|----|

**Legende:**

Ja: Die Signaturvariante ist für den Einsatzbereich erlaubt.

Nein: Die Signaturvariante ist für den Einsatzbereich nicht erlaubt.

Bedingt: Die Signaturvariante ist für den Einsatzbereich nicht erlaubt, es sei denn es wird durch eine **im Konnektor integrierte** Signaturreichtlinie explizit gefordert.

Die Spalten mit gelber Kopfzeile definieren die Signaturvarianten, die mit grauer, den Einsatzbereich. Beim Einsatzbereich wird zwischen nonQES und QES unterschieden und im Fall QES nach der Bereitstellung an der Außenschnittstelle oder intern für Fachmodule.

Die benötigten Signaturvarianten werden für XAdES über die Aufrufparameter IncludeObject und SignaturePlacement gemäß [OASIS-DSS] gesteuert.

Für CAdES erfolgt die Steuerung welche Signaturvariante gewählt wird, über den Aufrufparameter IncludeEContent.