
FinTS

Financial Transaction Services

- Schnittstellenspezifikation -

XML-Syntax

Herausgeber:

Bundesverband deutscher Banken e.V., Berlin

Deutscher Sparkassen- und Giroverband e.V., Bonn/Berlin

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Berlin

Bundesverband Öffentlicher Banken Deutschlands e.V., Berlin

Version: 4.0

Stand: 09.07.2004

Die vorliegende Schnittstellenspezifikation für eine automatisiert nutzbare multibankfähige Onlinebanking-Schnittstelle (im Folgenden: Schnittstellenspezifikation) wurde im Auftrag des Zentralen Kreditausschusses entwickelt. Sie wird hiermit zur Implementierung in Kunden- und Kreditinstitutssystemen freigegeben.

Die Schnittstellenspezifikation ist urheberrechtlich geschützt. Zur Implementierung in Kunden- und Kreditinstitutssystemen wird interessierten Herstellern unentgeltlich ein einfaches Nutzungsrecht eingeräumt. Im Rahmen des genannten Zwecks darf die Schnittstellenspezifikation auch - in unveränderter Form - vervielfältigt und zu den nachstehenden Bedingungen verbreitet werden.

Umgestaltungen, Bearbeitungen, Übersetzungen und jegliche Änderung der Schnittstellenspezifikation sind untersagt. Kennzeichnungen, Copyright-Vermerke und Eigentumsangaben dürfen in keinem Fall geändert werden.

Im Hinblick auf die Unentgeltlichkeit des eingeräumten Nutzungsrechts wird keinerlei Gewährleistung oder Haftung für Fehler der Schnittstellenspezifikation oder die ordnungsgemäße Funktion der auf ihr beruhenden Produkte übernommen. Die Hersteller sind aufgefordert, Fehler oder Auslegungsspielräume der Spezifikation, die die ordnungsgemäße Funktion oder Multibankfähigkeit von Kundenprodukten behindern, dem Zentralen Kreditausschuss zu melden. Es wird weiterhin ausdrücklich darauf hingewiesen, dass Änderungen der Schnittstellenspezifikation durch den Zentralen Kreditausschuss jederzeit und ohne vorherige Ankündigung möglich sind.

Eine Weitergabe der Schnittstellenspezifikation durch den Hersteller an Dritte darf nur unentgeltlich, in unveränderter Form und zu den vorstehenden Bedingungen erfolgen.

Dieses Dokument kann im Internet unter <http://www.fints.org> abgerufen werden

Versionsführung

Das vorliegende Dokument wurde von folgenden Personen erstellt bzw. geändert:

| Name | Organisation | Datum | Version | Dokumente | Anmerkungen |
|------|--------------|------------|-----------------------|------------------------------|-------------|
| | SIZ | 19.11.2003 | 4.0 final draft 01 | FinTS_4.0_XML- Syntax.doc | |
| | SIZ | 02.04.2004 | 4.0 final draft 02 | FinTS_4.0_XML- Syntax.doc | |
| | SIZ | 09.07.2004 | 4.0 | FinTS_4.0_XML- Syntax.doc | |

Änderungen gegenüber der Vorversion:

Änderungen sind im Dokument durch einen Randbalken markiert. Falls sich die Kapitelnummerierung geändert hat, bezieht sich die Kapitelangabe auf die neue Nummerierung.

| Ifd. Nr. | Kapitel | Kapitelnummer | Kennzeichnung ¹ | Art ² | Beschreibung |
|----------|-------------------------------|---------------------|----------------------------|------------------|---|
| 1 | Namensräume und Schema-Module | II.3 | | K | Segmentversionen der administrativen GV auf 1 gesetzt. |
| 2 | | II.4 | | K | Formale Grammatik zur Bildung von Geschäftsvorfall-Tags. |
| 3 | Nachrichtenaufbau | III.2, III.3, III.4 | | E | Gesamtrückmeldung zur Nachricht, Gesamtrückmeldung zur Auftragsliste. |
| 4 | | III.2.1.3 | | E | Produktidentifikation hinzu. |
| 5 | | III.3.4 b) | | E | Signatur-ID für digitale Signatur hinzu. |
| 6 | | III.4.1 | | K | Verwendung von Schlüsselnummer und -Version. |
| 7 | | III.4.1 a) | | E | Belegung Typ-Feld. |
| 8 | | III.4.3 a) | | F | Antwort enthält maximal zwei Schlüssel, Profilwechsel ist möglich |
| 9 | | III.4.4 | | Ä | Sperrung aus anderem Verfahren heraus ist möglich |
| 10 | | III.5 | | E | Umschließendes Element für Geschäftsvorfallparameter. |
| 11 | | III.5 b) | | Ä,E | BankID entfernt; HTTPS, SOAPHTTP hinzu. |
| 12 | | III.5 e) | | K | Typvorschrift für Parameterdaten. |
| 13 | | III.6 | | Ä | Name des Geschäftsvorfalles (ohne Version) statt Bezeichner (mit Version) in UPD. |
| 14 | | III.6 | | E | Benutzerparameter, Kontoparameter hinzu |
| 15 | | III.6.1, III.7.2.1 | | E | Abruf/Rückmeldung der Gast-UPD |
| 16 | | III.7 | | Ä | Administrative Aufträge: UserID hinzu, alle Versionsnummern auf 1 |
| 17 | | III.7.6.1 | | F | Rückmeldung Adressänderung korrigiert |
| 18 | | III.7.7.1 | | F | Auftrag Quittung korrigiert |
| 19 | Signierte Nachrichtenteile | IV.2.3 | | E | BankID, UDSDData hinzu in UserDefinedSignature |

¹ nur zur internen Zuordnung

² F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

| Ifd. Nr. | Kapitel | Kapitelnu mmer | Kennu ng ¹ | Art ² | Beschreibung |
|-------------|--|-------------------|--------------------------|------------------|---|
| 20 | Verschlüsselte und komprimierte Nachrichtenteile | V.1 | | K | Belegung von DDVKeyInfo, RDHKeyInfo. |

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 1 |

Inhaltsverzeichnis

| | |
|---|-----------|
| I. Einführung | 12 |
| II. Nachrichtensyntax..... | 13 |
| II.1 XML-Schemas..... | 14 |
| II.2 Zeichensatz und Kodierung | 15 |
| II.3 Namensräume und Schema-Module | 16 |
| II.3.1 Aufbau des Namensraum-URIs..... | 16 |
| II.3.2 Zuordnung der XML-Schemas zu den Namensräumen | 16 |
| II.3.3 Verwendung der Namensraum-Präfixe | 18 |
| II.4 Verbandseigene Geschäftsvorfälle | 20 |
| II.5 Komposition und Validierung einer FinTS-Nachricht..... | 22 |
| II.6 Kombierter Einsatz von FinTS mit anderen XML-Formaten | 24 |
| II.6.1 Anforderungen..... | 24 |
| II.6.2 Integration fremder Transaktionsformate in FinTS | 24 |
| II.6.3 Integration von FinTS-Nachrichten in Fremdformate | 25 |
| II.6.4 Integration von FinTS-Transaktionen in Fremdformate | 25 |
| II.7 FinTS-Datentypen | 26 |
| II.7.1 Binäre Daten..... | 26 |
| II.7.2 Transparente Daten..... | 26 |
| II.7.3 Status und Anzahl | 26 |
| II.7.4 Längenangaben..... | 26 |
| II.7.5 Aufzählungstypen | 27 |
| II.8 Referenzierung mit XPath-Ausdrücken | 28 |
| II.9 Symbole in den Schemadiagrammen | 31 |
| III. Nachrichtenaufbau | 33 |
| III.1 Überblick..... | 35 |
| III.2 Allgemeiner Aufbau von Benutzernachricht und Kreditinstitutsnachricht..... | 37 |
| III.2.1 Benutzernachricht..... | 37 |
| III.2.2 Kreditinstitutsnachricht | 41 |
| III.3 Verschiedene Benutzer- und Antwortnachrichten..... | 49 |
| III.3.1 Standard-Nachricht..... | 49 |
| III.3.2 Anonyme Nachricht | 50 |

| | | | | |
|----------|---|-----------|------------|--|
| Kapitel: | I | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 2 | Stand: | 09.07.2004 | Kapitel: Einführung |

| | | |
|--------------|--|------------|
| III.3.3 | Lebendmeldung | 52 |
| III.3.4 | Synchronisierung | 54 |
| III.4 | Keymanagement-Nachrichten | 56 |
| III.4.1 | Anforderung der Kreditinstitutsschlüssel | 56 |
| III.4.2 | Erstmalige Übermittlung eines Kundenschlüssels | 59 |
| III.4.3 | Schlüsseländerung | 62 |
| III.4.4 | Schlüsselsperrung | 65 |
| III.5 | Bankparameterdaten | 69 |
| III.6 | User-Parameterdaten | 76 |
| III.7 | Administrative Aufträge | 79 |
| III.7.1 | BPD | 79 |
| III.7.2 | UPD | 80 |
| III.7.3 | Intermediärszenarien | 82 |
| III.7.4 | PIN/TAN | 85 |
| III.7.5 | Abonnement | 90 |
| III.7.6 | Adressenregistrierung | 95 |
| III.7.7 | Quittung | 98 |
| III.7.8 | Verteile Signaturen | 99 |
| III.7.9 | Statusprotokoll | 103 |
| IV. | Signierte Nachrichtenteile | 106 |
| IV.1 | Überblick | 107 |
| IV.2 | Signaturtypen | 108 |
| IV.2.1 | [HBCI]-Verfahren: W3C-konforme XML-Signatur | 109 |
| IV.2.2 | PIN/TAN-Verfahren | 117 |
| IV.2.3 | Benutzerdefinierte Signatur | 118 |
| IV.3 | Botensignatur | 121 |
| IV.3.1 | W3C-konforme XML-Signatur | 122 |
| IV.3.2 | PIN/TAN-Verfahren | 124 |
| IV.3.3 | Benutzerdefinierte Signatur | 124 |
| IV.4 | Auftragssignatur | 125 |
| IV.4.1 | W3C-konforme XML-Signatur | 126 |
| IV.4.2 | PIN/TAN-Verfahren | 129 |
| IV.4.3 | Benutzerdefinierte Signatur | 129 |

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 3 |

| | |
|--|----------------|
| V. Verschlüsselte und komprimierte Nachrichtenteile | 130 |
| V.1 Aufbau des Verschlüsselungssegments | 131 |
| V.2 Verschlüsselung des Nachrichtenkörpers | 134 |
| V.3 Verschlüsselung von Aufträgen und Auftragsantworten | 135 |
| V.4 Komprimierung | 136 |
| VI. WEBSERVICES | 137 |
| VI.1 Webservices | 138 |
| VI.1.1 Einleitung..... | 138 |
| VI.1.2 SOAP..... | 140 |
| VI.1.3 WSDL | 142 |
| VII. Anhang: Konventionen zur Bildung von Elementnamen..... | 145 |

| | | | | |
|----------|---|----------|------------|--|
| Kapitel: | I | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | | | Dokument: XML-Syntax |
| Seite: | 4 | Stand: | 09.07.2004 | Kapitel: Einführung |

Abbildungsverzeichnis

| | |
|--|-----------|
| <i>Abbildung 1: Beispiel für eine Elementdeklaration</i> | <i>31</i> |
| <i>Abbildung 2: Beispiel für eine Typdefinition</i> | <i>31</i> |
| <i>Abbildung 3: Benutzernachricht</i> | <i>35</i> |
| <i>Abbildung 4: Kreditinstitutsnachricht</i> | <i>36</i> |
| <i>Abbildung 5: Nachrichtenkopf einer Benutzernachricht</i> | <i>38</i> |
| <i>Abbildung 6: Basistyp für die Nachrichtenkörper der Benutzernachricht</i> | <i>39</i> |
| <i>Abbildung 7: Initialisierung</i> | <i>40</i> |
| <i>Abbildung 8: Benutzerauftrag im abstrakten Basistyp der Auftragsliste.....</i> | <i>41</i> |
| <i>Abbildung 9: Nachrichtenkopf einer Kreditinstitutsnachricht</i> | <i>42</i> |
| <i>Abbildung 10: Basistyp für die Nachrichtenkörper der Kreditinstitutsnachricht</i> | <i>43</i> |
| <i>Abbildung 11: Initialisierungsantwort.....</i> | <i>44</i> |
| <i>Abbildung 12: Gesamtrückmeldung zur Nachricht</i> | <i>45</i> |
| <i>Abbildung 13: Rückmeldung zur Nachricht</i> | <i>45</i> |
| <i>Abbildung 14: Auftragsantwort</i> | <i>47</i> |
| <i>Abbildung 15: Standard-Benutzernachricht.....</i> | <i>49</i> |
| <i>Abbildung 16: Standard-Kreditinstitutsnachricht</i> | <i>50</i> |
| <i>Abbildung 17: Anonyme Benutzernachricht</i> | <i>51</i> |
| <i>Abbildung 18: Anonyme Kreditinstitutsnachricht</i> | <i>52</i> |
| <i>Abbildung 19: Benutzernachricht Lebendmeldung.....</i> | <i>53</i> |
| <i>Abbildung 20: Kreditinstitutsnachricht zur Lebendmeldung</i> | <i>53</i> |
| <i>Abbildung 21: Benutzernachricht Synchronisierung.....</i> | <i>54</i> |
| <i>Abbildung 22: Benutzerauftrag Synchronisierung</i> | <i>54</i> |
| <i>Abbildung 23: Kreditinstitutsnachricht zur Synchronisierung</i> | <i>55</i> |
| <i>Abbildung 24: Antwort auf eine Synchronisierung.....</i> | <i>55</i> |
| <i>Abbildung 25: Benutzernachricht Anforderung der Kreditinstitutsschlüssel</i> | <i>56</i> |
| <i>Abbildung 26: Anforderung öffentlicher Schlüssel.....</i> | <i>57</i> |

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 5 |

| | |
|---|-----------|
| <i>Abbildung 27: Kreditinstitutsnachricht Anforderung der Kreditinstitutsschlüssel.....</i> | <i>58</i> |
| <i>Abbildung 28: Öffentliche Schlüssellieferung.....</i> | <i>59</i> |
| <i>Abbildung 29: Benutzernachricht Übermittlung eines Kundenschlüssels</i> | <i>60</i> |
| <i>Abbildung 30: Einreichung öffentlicher Schlüssel</i> | <i>61</i> |
| <i>Abbildung 31: Kreditinstitutsnachricht zur Übermittlung eines Kundenschlüssels ...</i> | <i>62</i> |
| <i>Abbildung 32: Benutzernachricht Schlüsseländerung.....</i> | <i>63</i> |
| <i>Abbildung 33: Benutzerauftrag Schlüsseländerung</i> | <i>64</i> |
| <i>Abbildung 34: Kreditinstitutsnachricht zur Schlüsseländerung.....</i> | <i>65</i> |
| <i>Abbildung 35: Benutzernachricht Schlüsselsperrung.....</i> | <i>66</i> |
| <i>Abbildung 36: Benutzerauftrag Schlüsselsperrung</i> | <i>67</i> |
| <i>Abbildung 37: Kreditinstitutsnachricht zur Schlüsselsperrung.....</i> | <i>68</i> |
| <i>Abbildung 38: Bankparameterdaten</i> | <i>69</i> |
| <i>Abbildung 39: Allgemeine Bankparameterdaten</i> | <i>70</i> |
| <i>Abbildung 40: Kommunikationsparameter.....</i> | <i>70</i> |
| <i>Abbildung 41: Kommunikationsverfahren.....</i> | <i>71</i> |
| <i>Abbildung 42: Parameter der Sicherheitsverfahren</i> | <i>72</i> |
| <i>Abbildung 43: Sicherheitsverfahren RDH.....</i> | <i>72</i> |
| <i>Abbildung 44: Sicherheitsverfahren DDV.....</i> | <i>73</i> |
| <i>Abbildung 45: Sicherheitsverfahren OneTimePassword.....</i> | <i>73</i> |
| <i>Abbildung 46: Sicherheitsverfahren UserDefinedSignature</i> | <i>74</i> |
| <i>Abbildung 47: Komprimierungsverfahren</i> | <i>74</i> |
| <i>Abbildung 48: Geschäftsvorfallparameter</i> | <i>74</i> |
| <i>Abbildung 49: Parameterdaten.....</i> | <i>75</i> |
| <i>Abbildung 50: User-Parameterdaten.....</i> | <i>76</i> |
| <i>Abbildung 51: Allgemeine UPD</i> | <i>76</i> |
| <i>Abbildung 52: Kontoinformationen</i> | <i>77</i> |
| <i>Abbildung 53: Erlaubte Geschäftsvorfälle</i> | <i>78</i> |
| <i>Abbildung 54: Geschäftsvorfälle ohne Kontobezug</i> | <i>78</i> |

| | | | | |
|----------|---|----------|------------|--|
| Kapitel: | I | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | | | Dokument: XML-Syntax |
| Seite: | 6 | Stand: | 09.07.2004 | Kapitel: Einführung |

| | |
|--|-----------|
| <i>Abbildung 55: Benutzerauftrag BPD anfordern</i> | <i>79</i> |
| <i>Abbildung 56: Kreditinstitutsrückmeldung BPD anfordern</i> | <i>80</i> |
| <i>Abbildung 57: Bankparameterdaten BPD anfordern</i> | <i>80</i> |
| <i>Abbildung 58: Benutzerauftrag UPD anfordern</i> | <i>81</i> |
| <i>Abbildung 59: Kreditinstitutsrückmeldung UPD anfordern</i> | <i>81</i> |
| <i>Abbildung 60: Bankparameterdaten UPD anfordern</i> | <i>82</i> |
| <i>Abbildung 61: Benutzerauftrag Liste der Intermediäre</i> | <i>82</i> |
| <i>Abbildung 62: Kreditinstitutsrückmeldung Liste der Intermediäre</i> | <i>82</i> |
| <i>Abbildung 63: Bankparameterdaten Liste der Intermediäre</i> | <i>83</i> |
| <i>Abbildung 64: Benutzerauftrag Für einen Intermediär anmelden</i> | <i>83</i> |
| <i>Abbildung 65: Bankparameterdaten Für einen Intermediär anmelden</i> | <i>83</i> |
| <i>Abbildung 66: Benutzerauftrag Für einen Intermediär abmelden</i> | <i>84</i> |
| <i>Abbildung 67: Bankparameterdaten Für einen Intermediär abmelden</i> | <i>84</i> |
| <i>Abbildung 68: Benutzerauftrag UPDI ändern</i> | <i>84</i> |
| <i>Abbildung 69: Bankparameterdaten UPDI ändern</i> | <i>85</i> |
| <i>Abbildung 70: Benutzerauftrag PIN ändern</i> | <i>85</i> |
| <i>Abbildung 71: Bankparameterdaten PIN ändern</i> | <i>85</i> |
| <i>Abbildung 72: Benutzerauftrag TAN-Liste anfordern</i> | <i>86</i> |
| <i>Abbildung 73: Bankparameterdaten TAN-Liste anfordern</i> | <i>86</i> |
| <i>Abbildung 74: Benutzerauftrag TAN-Liste freischalten</i> | <i>87</i> |
| <i>Abbildung 75: Bankparameterdaten TAN-Liste freischalten</i> | <i>87</i> |
| <i>Abbildung 76: Benutzerauftrag PIN-Sperre</i> | <i>87</i> |
| <i>Abbildung 77: Bankparameterdaten PIN-Sperre</i> | <i>88</i> |
| <i>Abbildung 78: Benutzerauftrag PIN-Sperre aufheben</i> | <i>88</i> |
| <i>Abbildung 79: Bankparameterdaten PIN-Sperre aufheben</i> | <i>88</i> |
| <i>Abbildung 80: Benutzerauftrag TAN-Liste sperren/löschen</i> | <i>89</i> |
| <i>Abbildung 81: Bankparameterdaten TAN-Liste sperren/löschen</i> | <i>89</i> |
| <i>Abbildung 82: Benutzerauftrag TAN-Verbrauchsinformationen anfordern</i> | <i>89</i> |

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 7 |

| | |
|---|------------|
| <i>Abbildung 83: Kreditinstitutsrückmeldung TAN-Verbrauchsinformationen anfordern</i> | <i>90</i> |
| <i>Abbildung 84: Bankparameterdaten TAN-Verbrauchsinformationen anfordern</i> | <i>90</i> |
| <i>Abbildung 85: Benutzerauftrag Abonnement einreichen</i> | <i>91</i> |
| <i>Abbildung 86: Kreditinstitutsrückmeldung Abonnement einreichen</i> | <i>91</i> |
| <i>Abbildung 87: Bankparameterdaten Abonnement einreichen</i> | <i>92</i> |
| <i>Abbildung 88: Unterstützte Sicherheitsverfahren</i> | <i>93</i> |
| <i>Abbildung 89: Benutzerauftrag Abonnement löschen</i> | <i>94</i> |
| <i>Abbildung 90: Bankparameterdaten Abonnement löschen</i> | <i>94</i> |
| <i>Abbildung 91: Benutzerauftrag Abonnementsinformationen anfordern.....</i> | <i>94</i> |
| <i>Abbildung 92: Kreditinstitutsrückmeldung Abonnementsinformationen anfordern ...</i> | <i>95</i> |
| <i>Abbildung 93: Bankparameterdaten Abonnementsinformationen anfordern.....</i> | <i>95</i> |
| <i>Abbildung 94: Benutzerauftrag Adresse registrieren.....</i> | <i>96</i> |
| <i>Abbildung 95: Kreditinstitutsrückmeldung Adresse registrieren</i> | <i>96</i> |
| <i>Abbildung 96: Bankparameterdaten Adresse registrieren.....</i> | <i>96</i> |
| <i>Abbildung 97: Benutzerauftrag Adressregistrierungsinformationen holen</i> | <i>97</i> |
| <i>Abbildung 98: Kreditinstitutsrückmeldung Adressregistrierungsinformationen holen.....</i> | <i>97</i> |
| <i>Abbildung 99: Bankparameterdaten Adressregistrierungsinformationen holen</i> | <i>97</i> |
| <i>Abbildung 100: Benutzerauftrag Adressregistrierung löschen</i> | <i>98</i> |
| <i>Abbildung 101: Bankparameterdaten Adressregistrierung löschen</i> | <i>98</i> |
| <i>Abbildung 102: Benutzerauftrag Quittung</i> | <i>98</i> |
| <i>Abbildung 103: Bankparameterdaten Quittung</i> | <i>99</i> |
| <i>Abbildung 104: Benutzerauftrag Auftrag mit verteilten Signaturen einreichen.....</i> | <i>99</i> |
| <i>Abbildung 105: Kreditinstitutsrückmeldung Auftrag mit verteilten Signaturen einreichen</i> | <i>100</i> |
| <i>Abbildung 106: Bankparameterdaten Auftrag mit verteilten Signaturen einreichen</i> | <i>100</i> |
| <i>Abbildung 107: Benutzerauftrag Informationen zu Auftrag mit verteilten Signaturen</i> | <i>100</i> |

| | | | | |
|----------|---|----------|------------|--|
| Kapitel: | I | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | | | Dokument: XML-Syntax |
| Seite: | 8 | Stand: | 09.07.2004 | Kapitel: Einführung |

| | |
|--|------------|
| <i>Abbildung 108: Kreditinstitutsrückmeldung Informationen zu Auftrag mit verteilten Signaturen.....</i> | <i>101</i> |
| <i>Abbildung 109: Bankparameterdaten Informationen zu Auftrag mit verteilten Signaturen</i> | <i>101</i> |
| <i>Abbildung 110: Benutzerauftrag Auftrag mit verteilten Signaturen signieren.....</i> | <i>102</i> |
| <i>Abbildung 111: Kreditinstitutsrückmeldung Auftrag mit verteilten Signaturen signieren.....</i> | <i>102</i> |
| <i>Abbildung 112: Bankparameterdaten Auftrag mit verteilten Signaturen signieren .</i> | <i>102</i> |
| <i>Abbildung 113: Benutzerauftrag Auftrag mit verteilten Signaturen löschen</i> | <i>103</i> |
| <i>Abbildung 114: Bankparameterdaten Auftrag mit verteilten Signaturen löschen ...</i> | <i>103</i> |
| <i>Abbildung 115: Benutzerauftrag Statusprotokoll</i> | <i>104</i> |
| <i>Abbildung 116: Kreditinstitutsrückmeldung Statusprotokoll</i> | <i>104</i> |
| <i>Abbildung 117: Bankparameterdaten Statusprotokoll</i> | <i>105</i> |
| <i>Abbildung 118: Signatur einer Benutzernachricht.....</i> | <i>108</i> |
| <i>Abbildung 119: Signatur einer Kreditinstitutsnachricht.....</i> | <i>108</i> |
| <i>Abbildung 120: Element Signature</i> | <i>109</i> |
| <i>Abbildung 121: Element Reference.....</i> | <i>111</i> |
| <i>Abbildung 122: Element RDHKeyInfo</i> | <i>112</i> |
| <i>Abbildung 123: Element DDVKeyInfo.....</i> | <i>113</i> |
| <i>Abbildung 124: Element RDHProperty</i> | <i>115</i> |
| <i>Abbildung 125: Element DDVProperty</i> | <i>116</i> |
| <i>Abbildung 126: Element OneTimePassword.....</i> | <i>117</i> |
| <i>Abbildung 127: Element OneTimePasswordReply.....</i> | <i>118</i> |
| <i>Abbildung 128: Element UserDefinedSignature</i> | <i>119</i> |
| <i>Abbildung 129: Botensignatur im Nachrichtenkörper einer Benutzernachricht</i> | <i>121</i> |
| <i>Abbildung 130: Botensignatur im Nachrichtenkörper der Kreditinstitutsnachricht..</i> | <i>122</i> |
| <i>Abbildung 131: Auftragssignatur in einer Benutzernachricht</i> | <i>125</i> |
| <i>Abbildung 132: Auftragssignatur in einer Kreditinstitutsnachricht</i> | <i>126</i> |
| <i>Abbildung 133: Verschlüsselung mit dem EncryptedData-Element</i> | <i>131</i> |
| <i>Abbildung 134: Verschlüsselter Sitzungsschlüssel</i> | <i>132</i> |

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 9 |

| | |
|---|------------|
| <i>Abbildung 135: Verschlüsselung des Nachrichtenkörpers der Benutzernachricht.....</i> | <i>134</i> |
| <i>Abbildung 136: Verschlüsselung des Nachrichtenkörpers der Kreditinstitutsnachricht</i> | <i>134</i> |
| <i>Abbildung 137: Auftragsverschlüsselung in der Standard-Benutzernachricht</i> | <i>135</i> |
| <i>Abbildung 138: Auftragsverschlüsselung in der Standard-Kreditinstitutsnachricht</i> | <i>135</i> |
| <i>Abbildung 139: Webservice Beispiel</i> | <i>138</i> |
| <i>Abbildung 140: Webservice Schichtenmodell</i> | <i>139</i> |
| <i>Abbildung 141: Transport einer FinTS-Nachricht mit SOAP</i> | <i>141</i> |

| | | |
|---------------|----------------------|--|
| Kapitel: I | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 10 | Stand: 09.07.2004 | Kapitel: Einführung |

Literaturverzeichnis

- [Canonical XML] Canonical XML Version 1.0, W3C Recommendation 15 March 2001, <http://www.w3.org/TR/xml-c14n>
- [DataDictionary] Financial Transaction Services (FinTS) – Data Dictionary, Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss
- [Exclusive XML Canonicalization] Exclusive XML Canonicalization Version 1.0, W3C Recommendation 18 July 2002, <http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/>
- [Formals] Financial Transaction Services (FinTS) – Formals (Allgemeine Festlegungen für multibankfähige Online-Verfahren der deutschen Kreditwirtschaft), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss
- [HBCI] Financial Transaction Services (FinTS) – Security (Sicherheitsverfahren HBCI), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss
- [Messages] Financial Transaction Services (FinTS) – Messages (Multibankfähige Geschäftsvorfälle), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss
- [Namespaces] Namespaces in XML, W3C Recommendation 14 January 1999, <http://www.w3.org/TR/REC-xml-names/>
- [PINTAN] Financial Transaction Services (FinTS) – Security (Sicherheitsverfahren PIN/TAN), Version 4.0 final draft 02, 02.04.2004, Zentraler Kreditausschuss
- [RFC1951] DEFLATE Compressed Data Format Specification version 1.3, <http://www.ietf.org/rfc/rfc1951.txt>
- [S.W.I.F.T.] <http://www.swift.com>
- [SOAP 1] SOAP Version 1.2 Part 1: Messaging Framework, W3C Recommendation 24 June 2003, <http://www.w3.org/TR/2003/REC-soap12-part1-20030624/>
- [SOAP 2] SOAP Version 1.2 Part 2: Adjuncts, W3C Recommendation 24 June 2003, <http://www.w3.org/TR/2003/REC-soap12-part2-20030624/>
- [WSDL 1] Web Services Description Language (WSDL) Version 2.0, Part 1: Core Language, W3C Working Draft 10 November 2003, <http://www.w3.org/TR/2003/WD-wsdl20-20031110>
- [WSDL 2] Web Services Description Language (WSDL) Version 2.0, Part 2: Message Patterns, W3C Working Draft 10 November 2003, <http://www.w3.org/TR/2003/WD-wsdl20-patterns-20031110>

| | | |
|--|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: I |
| Kapitel: Einführung | Stand: 09.07.2004 | Seite: 11 |

- [WSDL 3] Web Services Description Language (WSDL) Version 1.2, Part 3: Bindings, W3C Working Draft 11 June 2003, <http://www.w3.org/TR/2003/WD-wsdl12-bindings-20030611>
- [XML1.0] Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation 6 October 2000, <http://www.w3.org/TR/2000/REC-xml-20001006>
- [XML Encryption] XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002, <http://www.w3.org/TR/xmlenc-core/>
- [XML Schema 1] XML Schema Part 1: Structures, W3C Recommendation 2 May 2001, <http://www.w3.org/TR/xmlschema-1/>
- [XML Schema 2] XML Schema Part 2: Datatypes, W3C Recommendation 2 May 2001, <http://www.w3.org/TR/xmlschema-2/>
- [XML Signature] XML-Signature Syntax and Processing, W3C Candidate Recommendation 19 April 2001, <http://www.w3.org/TR/xmldsig-core/>
- [XPath] XML Path Language (XPath) Version 1.0, W3C Recommendation 16 November 1999, <http://www.w3.org/TR/1999/REC-xpath-19991116>
- [XPath Filter] XML-Signature XPath Filter 2.0, W3C Recommendation 08 November 2002, <http://www.w3.org/TR/xmldsig-filter2/>

| | | | | |
|----------|----|-----------|------------|--|
| Kapitel: | I | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 12 | Stand: | 09.07.2004 | Kapitel: Einführung |

I. EINFÜHRUNG

Dieses Dokument beschreibt im ersten Teil „Nachrichtensyntax“ die allgemeinen Anforderungen an das XML-Format von FinTS-Nachrichten. Die Anforderungen sind Einschränkungen in der Benutzung der XML-Standards, die in FinTS angewendet werden. Hier wird FinTS mit den folgenden XML-Standards in Beziehung gesetzt:

- mit dem XML-Basisstandard ([XML 1.0]),
- der Verwendung von Namensräumen ([Namespaces]),
- der Validierung durch XML-Schemas ([XML Schema 1], [XML Schema 2]) und
- der Referenzierung von Nachrichtenelementen mit XPath-Ausdrücken ([XPath]).

Im zweiten Teil „Nachrichtenaufbau“ werden die XML-Datenformate der FinTS-Nachrichten in detaillierter Form dokumentiert. In diesem Abschnitt geht es um anwendungsunabhängige XML-Konventionen für FinTS. Diese Konventionen gelten auch für verbandsspezifische Erweiterungen von FinTS.

Grafiken stellen die Struktur der zugrunde liegenden FinTS-Schemas zum allgemeinen Nachrichtenaufbau und zu den administrativen Geschäftsvorfällen dar. Im Text sind zu den einzelnen Elementen Belegungsrichtlinien angegeben, sofern sie über die im [DataDictionary] vorhandenen Erläuterungen hinausgehen.

Die Abschnitte drei und vier befassen sich mit den Sicherheitsmechanismen von XML. Dazu gehören

- das Signieren ([XML Signature]),
- die Referenzierung mit XPath-Ausdrücken in einer Signatur ([XPath Filter]),
- die Kanonisierung ([Canonical XML], [Exclusive Canonical XML]) und
- das Verschlüsseln ([XML Encryption])

von FinTS-Nachrichten.

Die Kompression von FinTS-Nachrichtenteilen wird als eine spezielle Form der Verschlüsselung betrachtet. Für beide Verfahren wird der [XML Encryption]-Standard angewendet.

Der letzte Abschnitt beschreibt den Einsatz von Webservices im Zusammenhang mit FinTS. Die referenzierten Webservice Standards des W3C werden

- als Übertragungsprotokoll ([SOAP 1], [SOAP 2])
- und zur Definition der FinTS-Webservices ([WSDL 1], [WSDL 2])

eingesetzt. Für den Einsatz beider Standards im Zusammenhang mit FinTS werden Beispiele gezeigt.

Alle vorangehend genannten XML-Standards wurden vom W3C (World Wide Web Consortium) normiert. Die üblicherweise von XML-Implementierungen unterstützten Sicherheitsverfahren des W3C werden allerdings durch die [HBCI]-Sicherheitsverfahren erweitert.

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: XML-Schemas | Stand: 09.07.2004 | Seite: 13 |

II. NACHRICHTENSYNTAX

| | |
|---|-----------|
| II.1 XML-Schemas..... | 14 |
| II.2 Zeichensatz und Kodierung | 15 |
| II.3 Namensräume und Schema-Module | 16 |
| II.3.1 Aufbau des Namensraum-URIs..... | 16 |
| II.3.2 Zuordnung der XML-Schemas zu den Namensräumen | 16 |
| II.3.3 Verwendung der Namensraum-Präfixe | 18 |
| II.4 Verbandseigene Geschäftsvorfälle | 20 |
| II.5 Komposition und Validierung einer FinTS-Nachricht..... | 22 |
| II.6 Kombierter Einsatz von FinTS mit anderen XML-Formaten | 24 |
| II.6.1 Anforderungen..... | 24 |
| II.6.2 Integration fremder Transaktionsformate in FinTS | 24 |
| II.6.3 Integration von FinTS-Nachrichten in Fremdformate | 25 |
| II.6.4 Integration von FinTS-Transaktionen in Fremdformate..... | 25 |
| II.7 FinTS-Datentypen | 26 |
| II.7.1 Binäre Daten..... | 26 |
| II.7.2 Transparente Daten..... | 26 |
| II.7.3 Status und Anzahl | 26 |
| II.7.4 Längenangaben..... | 26 |
| II.7.5 Aufzählungstypen..... | 27 |
| II.8 Referenzierung mit XPath-Ausdrücken | 28 |
| II.9 Symbole in den Schemadiagrammen | 31 |

| | | |
|----------------|----------------------|--|
| Kapitel: II | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 14 | Stand: 09.07.2004 | Kapitel: Nachrichtensyntax Abschnitt: XML-Schemas |

II.1 XML-Schemas

Die FinTS-Nachrichten werden in XML-Syntax anhand von XML-Schemas spezifiziert.



Die syntaktische Prüfung und die Schema-Validierung einer FinTS-Nachricht erfolgt durch einen XML-Parser. Der validierende XML-Parser muss XML-Schemas gemäß [XML Schema 1] bzw. [XML Schema 2] unterstützen.



Whitespace in FinTS-Nachrichten ist signifikant.



Bei XML-Parsern kann die Behandlung von Whitespace üblicherweise konfiguriert werden. Die XML-Parser und alle Komponenten einer Anwendung müssen FinTS-Nachrichten so verarbeiten, dass Whitespace erhalten bleibt.



| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Zeichensatz und Kodierung | Stand: 09.07.2004 | Seite: 15 |

II.2 Zeichensatz und Kodierung

Der Zeichensatz zur Verarbeitung eines XML-Dokuments wird durch das *encoding*-Attribut der XML-Verarbeitungsanweisung (processing instruction) festgelegt, die in der ersten Zeile eines XML-Dokuments steht.

```
<?xml version="1.0" encoding="utf-8"?>
```

Die Verarbeitungsanweisung muss sich in allen FinTS-Dokumenten und allen zugehörigen Schema-Dokumenten befinden, um eine ordnungsgemäße Verarbeitung zu gewährleisten. Alle XML-Dokumente, die FinTS-Nachrichten enthalten, müssen im Unicode-Format [UTF-8] kodiert werden. FinTS-Nachrichten in anderen Kodierungen sind nicht zulässig.



Auch die Entwicklungswerkzeuge und XML-basierte Anwendungen für FinTS-Nachrichten (z. B. XSLT-Stylesheets) müssen die Kodierung [UTF-8] verwenden, um Fehler bei der Abbildung zwischen verschiedenen Zeichensätzen zu vermeiden.

Für FinTS-Nachrichten, die in XML serialisiert werden, wird der in XML übliche Kodierungsmechanismus verwendet. In XML müssen die für die Auszeichnung verwendeten Zeichen &, <, >, ' und " kodiert werden. Die Zeichen werden in XML mit den sogenannten allgemeinen Entitäten (entities) *&*, *<*, *>*, *'* und *"* dargestellt. Dies sind vordefinierte Zeichen-Entitäten (character entities), die nicht in einem Schema deklariert werden müssen.

Beispiel:

vor Entwertung (kein wohlgeformtes XML):

```
Betrag > EUR 1000
```

nach Entwertung (wohlgeformtes XML):

```
Betrag &gt; EUR 1000
```

| | | |
|----------------|----------------------|---|
| Kapitel: II | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 16 | Stand: 09.07.2004 | Kapitel: Nachrichtensyntax Abschnitt: Namensräume und Schema-Module |

II.3 Namensräume und Schema-Module

Namensräume ([Namespaces]) werden zur Vermeidung von Namenskonflikten in XML-Dokumenten eingesetzt. Darüber hinaus werden sie in den XML-Schemas zur Validierung der XML-Dokumente verwendet, um eindeutige Deklaration von Elementen und eindeutige Definitionen von Typen zu gewährleisten.

In FinTS legen Namensräume die Ebene (Nachrichten- oder Transaktionsebene) eines Bezeichners in einer FinTS-Nachricht fest. Außerdem erleichtern die FinTS-Namensräume die Wiederverwendung von Schemakomponenten außerhalb von FinTS.

II.3.1 Aufbau des Namensraum-URIs

Die Namensräume werden entsprechend dem W3C-Standard [Namespaces] durch die Zuordnung eines URI zu einem Namensraum-Präfix bzw. durch die Zuordnung des URI zum voreingestellten Namensraum (default namespace) definiert.

Die URIs für die ZKA-weit gültigen Namensräume von FinTS besitzen den folgenden Aufbau:

```
<Domain>/spec/<Schematyp>/<Version>/<Release>/<Modulverzeichnis>
```

- Die Domain ist der feste Wert *http://www.fints.org/*
- Der Schematyp ist *xmlschema* für XML-Schemas (andere Schematypen werden derzeit nicht unterstützt).
- Die Versionsnummer entspricht der FinTS-Version. Zur Unterscheidung der Nachbesserungen (patches) einer FinTS-Version wird das entsprechende Releasedatum im Format *pJJJJMMTT* in den Namensraum-URI übernommen.
- Das Release ist *final* bzw. *p<Datum des Patches>*.

Beispiele:

```
http://www.fints.org/spec/xmlschema/4.0/final/transactions
http://www.fints.org/spec/xmlschema/4.0/p20010817/transactions
```

II.3.2 Zuordnung der XML-Schemas zu den Namensräumen

In FinTS werden derzeit zwei Namensräume verwendet.

- FinTS-Typen (Modulverzeichnis: *types*) und
- FinTS-Transaktionen (Modulverzeichnis: *transactions*)

Dem Namensraum für den allgemeinen Nachrichtenaufbau (FinTS-Typen) werden alle Schemas zugeordnet, die wiederverwendbare Komponenten enthalten oder generell den Aufbau einer FinTS-Nachricht beschreiben.

Beispiel:

```
<xs:schema
  targetNamespace="http://www.fints.org/spec/xmlschema/4.0/final/types"
  ...
```

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Namensräume und Schema-Module | Stand: 09.07.2004 | Seite: 17 |

Die zugehörigen XML-Schemas sind gemäß ihrer Semantik in mehrere Module unterteilt:

| Schemadatei | Inhalt |
|----------------|---|
| common.xsd | allgemeine abstrakte Basistypen und häufig verwendete Komponenten |
| formats.xsd | Basisformate und abgeleitete Formate |
| message.xsd | Grundgerüst des Nachrichtenaufbaus |
| paramdata.xsd | Typdefinitionen für Bank- und User-Parameterdaten |
| patterns.xsd | häufig verwendete bankfachliche Typen |
| structures.xsd | Definitionen und Deklarationen für administrative Nachrichtentypen und -komponenten |

Die Bestandteile zur Definition von Geschäftsvorfällen (Benutzeraufträge, Kreditinstitutsrückmeldungen und Bankparameterdaten) sind dem Namensraum für FinTS-Transaktionen zugeordnet:

Beispiel:

```
<xs:schema
  targetNamespace="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
  ...
```

Die folgende Liste zeigt die Schema-Module der administrativen Geschäftsvorfälle in FinTS:

| Schemadatei | Inhalt |
|--------------------------|--|
| AddReg-1.xsd | Adressenregistrierung |
| AddRegDelete-1.xsd | Adressenregistrierung löschen |
| AddRegInfo-1.xsd | Adressenregistrierungsinformationen |
| BankParamData-1.xsd | Bankparameterdaten anfordern |
| BlockPIN-1.xsd | PIN sperren |
| ChangePIN-1.xsd | PIN ändern |
| DistSigsDelete-1.xsd | Auftrag mit verteilten Signaturen löschen |
| DistSigsInfo-1.xsd | Informationen zu Auftrag mit verteilten Signaturen |
| DistSigsSign-1.xsd | Auftrag mit verteilten Signaturen signieren |
| DistSigsSubmit-1.xsd | Auftrag mit verteilten Signaturen einreichen |
| InterList-1.xsd | Liste der Intermediäre |
| InterSignOff-1.xsd | Beim Intermediär abmelden |
| InterSignOn-1.xsd | Beim Intermediär anmelden |
| Receipt-1.xsd | Quittung |
| RevokePINBlock-1.xsd | PIN-Sperre aufheben |
| StatProt-1.xsd | Statusprotokoll |
| Subscription-1.xsd | Abonnement einreichen |
| SubscriptionDelete-1.xsd | Abonnement löschen |
| SubscriptionInfo-1.xsd | Abonnementsinformationen anfordern |
| TANList-1.xsd | TAN-Liste anfordern |
| TANListBlock-1.xsd | TAN-Liste löschen |
| TANListDisplay-1.xsd | TAN-Verbrauchsinformationen anfordern |
| TANListEnable-1.xsd | TAN-Liste freischalten |
| UPDIEdit-1.xsd | UPDI ändern |
| UserParamData-1.xsd | User-Parameterdaten anfordern (UPD) |

Die allgemeinen ZKA-weit definierten Geschäftsvorfälle finden sich in [Messages].

| | | | | |
|----------|----|----------|------------|---|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | | | Dokument: XML-Syntax |
| Seite: | 18 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax |
| | | | | Abschnitt: Namensräume und Schema-Module |

II.3.3 Verwendung der Namensraum-Präfixe

Bei der Verwendung von Namensräumen in XML-Dokumenten kann entweder der voreingestellte Namensraum belegt werden oder es können beliebige Präfixe definiert werden, die einen Namensraum repräsentieren.

In einer FinTS-Nachricht sollte der voreingestellte Namensraum immer mit dem Namensraum für den allgemeinen Nachrichtenaufbau (FinTS-Typen) belegt werden, weil sich dadurch die Schreibweise der Elemente verkürzt. Zur Belegung des voreingestellten Namensraumes wird dem Attribut *xmlns* der entsprechende Namensraum-URI zugewiesen.

Beispiel:

```
<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  ...
</ReqMsg>
```

Zum Vergleich das Beispiel ohne die Verwendung eines voreingestellten Namensraumes:

```
<fintstype:ReqMsg
  xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types">
  ...
</fintstype:ReqMsg>
```

Hier wird das Präfix *fintstype* durch das Attribut *xmlns:fintstype* mit dem Namensraum-URI für FinTS-Typen belegt. Das Präfix muss in diesem Beispiel allen FinTS-Elementen vorangestellt werden, die den allgemeinen Nachrichtenaufbau beschreiben.

Um für FinTS eine eindeutige leicht verständliche Vergabe von Präfixen zu gewährleisten, wird empfohlen, dass als Präfix-Bezeichner

- *fintstype* für den allgemeinen Nachrichtenaufbau und
- *fintstrans* für Transaktionen

verwendet werden.



Da der voreingestellte Namensraum bereits mit dem URI für FinTS-Typen belegt ist, entfällt in XML-Dokumenten die Notwendigkeit der Verwendung des Präfixes *fintstype*. Dieses Präfix sollte ausschließlich in Schema-Modulen zur Definition von verbandsspezifischen Typen und Geschäftsvorfällen verwendet werden (siehe II.4 Verbandseigene Geschäftsvorfälle).

Im folgenden Beispiel werden der voreingestellte Namensraum und das Präfix *fintstrans* für eine Einzelüberweisung (*SingRemitt*) definiert:

```
<fintstrans:SingRemitt_1_Req
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions">
  ...
</fintstrans:SingRemitt_1_Req>
```

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Namensräume und Schema-Module | Stand: 09.07.2004 | Seite: 19 |

Das Element *SingRemitt_1_Req* ist im Namensraum für FinTS-Transaktionen deklariert. Deshalb wird für dieses Element das Präfix *fintstrans* verwendet. Für allgemeine Datenstrukturen, die in der Einzelüberweisung vorkommen, muss kein Präfix definiert werden, da der voreingestellte Namensraum (FinTS-Typen) an die eingeschachtelten Elemente vererbt wird. Analog zum voreingestellten Namensraum vererben sich auch die Präfix-Deklarationen auf die, in der Deklaration geschachtelten Datenstrukturen.

| | | | | |
|----------|----|------------|-----------------------|--|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 20 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax |
| | | Abschnitt: | Verbandseigene | Geschäftsvorfälle |

II.4 Verbandseigene Geschäftsvorfälle

Die Unterscheidung zwischen ZKA-weit definierten und verbandsspezifischen Geschäftsvorfällen erfolgt ebenfalls durch die Verwendung von Namensräumen. Für verbandseigene von FinTS abgeleitete Schemas müssen eigene Namensräume definiert werden.

Die URIs für die verbandseigenen Namensräume werden in FinTS nicht festgelegt. Sie sollten sich aber an dem oben (siehe *II.3.1 Aufbau des Namensraum-URIs*) beschriebenen Konzept orientieren:

```
<Verbands-Domain>/spec/<Schematyp>/<Version>/<Release>/<Modulverzeichnis>
```

Schemas für verbandseigene Geschäftsvorfälle werden im jeweiligen Namensraum für Transaktionen abgelegt. Eine verbandsweit abweichende Verwendung der Unterteilung in die beiden Namensräume Typen und Transaktionen ist nicht zulässig. Die Schema-Module sollten immer in dem durch den Namensraum-URI spezifizierten Unterverzeichnis abgelegt werden.

Beispiel:

Die *xy-bank* könnte einen selbstdefinierten Geschäftsvorfall *t* unter dem Namensraum-URI

```
http://www.xy-bank.org/spec/xmlschema/4.0/final/transactions
```

als Schema unter dem URI

```
http://www.xy-bank.org/spec/xmlschema/4.0/final/transactions/t.xsd
```

ablegen und in den XML-Dokumenten das Präfix

```
xmlns:fintstrans-xy="http://www.xy-bank.org/spec/xmlschema/4.0/final/transactions"
```

verwenden.

Für verbandseigene von FinTS abgeleitete Schemas sollten der besseren Lesbarkeit wegen eigene Namensraum-Präfixe definiert werden. Die Präfixe sollten mit *fintstype-* bzw. *fintstrans-* beginnen, um zu verdeutlichen, dass von einem FinTS-Nachrichtenformat abgeleitet wurde.

Beispiele:

- BdB: *fintstype-b*, *fintstrans-b*
- BVR: *fintstype-g*, *fintstras-g*
- DSGV: *fintstype-s*, *fintstrans-s*
- VÖB: *fintstype-v*, *fintstrans-v*

Die XML-Elemente für Benutzerauftrag, Kreditinstitutsantwort und Bankparameterdaten eines Geschäftsvorfalles sind grundsätzlich im selben Namensraum zu definieren. Die Benennung ist einheitlich anhand des folgenden Schemas vorzunehmen:

Benutzerauftrag:

```
XMLTag ::= ID 'Req'
```

Kreditinstitutsrückmeldung:

```
XMLTag ::= ID 'Resp'
```

Bankparameterdaten:

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Verbandseigene Geschäftsvorfälle | Stand: 09.07.2004 | Seite: 21 |

```
XMLTag ::= ID ' Par'
```

mit:

```
ID      ::= Name ' ' Version
Name    ::= NCName
Version ::= [1-9] ([0-9]) *
```

Beispiel: Einzelüberweisung (SingRemitt) Version 1

```
SingRemitt 1 Req
SingRemitt 1 Resp
SingRemitt 1 Par
```

Die Systematik ermöglicht u. a. die Zuordnung der Bankparameterdaten zu Geschäftsvorfällen, ohne zusätzliche Zuordnungstabellen.

Hinweis:

Die formale Grammatik verwendet eine einfache *Extended Backus-Naur Form* (EBNF), wie sie im [XML1.0] beschrieben ist. Das verwendete Nichtterminal *NCName* ist in [Namespaces] beschrieben.

| | | | | |
|----------|----|----------|------------|---|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: | 22 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax Abschnitt: Komposition und Validierung einer FinTS-Nachricht |

II.5 Komposition und Validierung einer FinTS-Nachricht

FinTS-Nachrichten müssen gemäß der Schema-Validierung nach [XML Schema 1] bzw. [XML Schema 2] validiert werden.

Zur Validierung von FinTS-Nachrichten müssen diese im Namensraum für FinTS-Typen deklariert sein. Die eingebetteten Geschäftsvorfälle müssen im Namensraum für FinTS-Transaktionen oder in den Namensräumen der verbandsspezifischen Geschäftsvorfälle deklariert sein. Dazu sind auf der Nachrichtenebene und auf der Transaktionsebene die entsprechenden Schemas mit dem Attribut *schemaLocation* zuzuordnen. Das Attribut *schemaLocation* ist im Namensraum für Instanzen von XML-Schemas <http://www.w3.org/2001/XMLSchema-instance> definiert. Deshalb wird dem Attribut *schemaLocation* das entsprechend deklarierte Präfix *xsi* vorangestellt.

Das Attribut *schemaLocation* enthält als Wertepaar den Zielnamensraum (*targetNamespace*), dem die Schemas zugeordnet sind, sowie den URL auf das zugeordnete Schema-Dokument. Beide Werte sind durch ein Leerzeichen getrennt.

Beispiel:

```
<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/final/types
    http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd">
  ...
  <Orders>
    <fintstrans:SingRemitt
      xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
      xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/final/transactions
        http://www.fints.org/spec/xmlschema/4.0/final/transactions/SingRemitt-4.xsd">
      ...
    </fintstrans:SingRemitt>
  </Orders>
  ...
</ReqMsg>
```

Im Beispiel wird eine Einzelüberweisung als Auftrag in eine Benutzernachricht eingebettet. Die Benutzernachricht kann mit Ausnahme der enthaltenen Geschäftsvorfälle durch die Angabe eines einzigen Schemas (<http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd>) validiert werden.

Für jeden Geschäftsvorfall existiert ein eigenes Schema-Dokument zur Validierung. Im Beispiel wird daher dem eingebetteten Geschäftsvorfall das Schema <http://www.fints.org/spec/xmlschema/4.0/final/transactions/SingRemitt-4.xsd> zur Validierung zugeordnet.

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Komposition und Validierung einer FinTS-Nachricht | Stand: 09.07.2004 | Seite: 23 |



Normalerweise ist es effizienter, die FinTS-Schemas zur Validierung lokal zu speichern. Bei der lokalen Speicherung der Schemas sollte der Verzeichnispfad nach der FinTS-Domain (siehe *II.3.1 Aufbau des Namensraum-URIs*) erhalten bleiben.



Wenn ein System lokal gespeicherte Schemas verwendet, wird es evtl. auch in der zu sendenden FinTS-Nachricht diese lokale Schema-Adresse angeben (siehe nachfolgendes Beispiel).

Die jeweils empfangende Seite wird die lokalen Schema-Adressen der sendenden Seite im Allgemeinen nicht auflösen können. Es wird insbesondere für die Kreditinstitutsseite grundsätzlich empfohlen, die Schema-Adresse im Dokument zu ignorieren und die lokal gespeicherten Schemas anhand geeigneter Mechanismen selbstständig zu identifizieren.

Beispiel mit lokalen Schema-Adressen:

```
<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/final/types
    c:/fints/spec/xmlschema/4.0/final/types/message.xsd">
  ...
  <Orders>
    <fintstrans:SingRemitt_1_Req
      xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
      xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/final/transactions
        c:/fints/spec/xmlschema/4.0/final/transactions/SingRemitt-4.xsd">
      ...
    </fintstrans:SingRemitt_1_Req>
  </Orders>
  ...
</ReqMsg>
```

| | | | | |
|----------|----|------------|--|--|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 24 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax |
| | | Abschnitt: | Kombinierter Einsatz von FinTS mit anderen XML-Formaten | |

II.6 Kombiniertes Einsatz von FinTS mit anderen XML-Formaten

FinTS lässt sich durch die Verwendung von Namensräumen in Kombination mit anderen XML-Formaten einsetzen, so dass Namenskonflikte bei der Verarbeitung leicht aufgelöst werden können. Dazu bieten sich vielfältige Möglichkeiten. Der folgende Abschnitt zeigt die Anforderungen an die in Kombination mit FinTS verwendeten Fremdformate.

II.6.1 Anforderungen

Bei den Anforderungen handelt es sich um Empfehlungen, die zur Modularisierung, Robustheit und einfachen Wartbarkeit von XML-Anwendungen beitragen.

XML-Schemas erlauben die Validierung von Teilen eines XML-Dokuments gegen mehrere verschiedene Schemas. Somit können XML-Nachrichten in heterogenen Formaten typischer in einem einzigen XML-Dokument transportiert werden.

Wenn XML-Fremdformate in Kombination mit FinTS eingesetzt werden, dann sollten deren Typdefinitionen und Deklarationen in einem separaten Namensraum vorgenommen werden. Dadurch können die Anwendungen bei der Verarbeitung der XML-Dokumente eindeutig entscheiden, welchem Nachrichtenformat ein XML-Fragment zuzuordnen ist. Außerdem sollte eindeutig festgelegt werden, wie die XML-Dokumente zu validieren sind.

Falls in einem XML-Dokument FinTS-Nachrichten mit anderen Nachrichtentypen (z. B. S.W.I.F.T.-Nachrichten) gemischt werden (siehe *II.6.3 Integration von FinTS-Nachrichten in Fremdformate*), sollte der voreingestellte Namensraum für die FinTS-fremden Datenstrukturen mit einem zum Fremdformat passenden Namensraum-URI belegt werden.

Falls das Fremdformat nicht in einem Namensraum definiert wurde, ist der voreingestellte Namensraum auf den Standardwert zurückzusetzen:

```
<Fremdformat xmlns="">
...
</Fremdformat>
```

II.6.2 Integration fremder Transaktionsformate in FinTS

FinTS-Nachrichten erlauben die Integration von Geschäftsvorfällen in Fremdformaten an bestimmten dafür vorgesehenen Stellen im Nachrichtenaufbau. An diesen Stellen sind in den XML-Schemas von FinTS beliebige Elemente des XML-Schematyps *any* vorhanden.

Beispiel:

```
<xs:any namespace="##any" processContents="lax"/>
```

An den Stellen, wo Fremdformate in die FinTS-Nachricht integriert werden können, werden sie validiert, sofern der Parser in der Lage ist, dies zu tun (Attribut *processContents="lax"*).

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Kombinierter Einsatz von FinTS mit anderen XML-Formaten | Stand: 09.07.2004 | Seite: 25 |

Im folgenden Beispiel wird ein [S.W.I.F.T.]-Geschäftsvorfall in eine FinTS-Nachricht integriert:

```
<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/
    fints/spec/xmlschema/4.0/final/types/message.xsd">
  ...
  <Orders>
    <XctCpfSTPPlusBlkCtTrf
      xmlns="<S.W.I.F.T. Namensraum>"
      xsi:schemaLocation="<S.W.I.F.T. Namensraum> XctCpfSTPPlusBlkCtTrf.xsd">
      ...
    </XctCpfSTPPlusBlkCtTrf>
  </Orders>
</ReqMsg>
```

An der Stelle *<S.W.I.F.T. Namensraum>* ist der zum [S.W.I.F.T.]-Geschäftsvorfall gehörende Namensraum-URI einzustellen.

II.6.3 Integration von FinTS-Nachrichten in Fremdformate

FinTS-Nachrichten können unter Erhaltung einer syntaktisch korrekten XML-Struktur des Gesamtdokumentes in ein XML-Dokument eingebettet werden. Damit bleiben sie beim Mischen von Fremdformaten mit FinTS-Nachrichten als eindeutig validierbare Einheit erhalten.

Der Namensraum der FinTS-Nachrichten macht diese im Bezug zum übrigen Dokument unterscheidbar. Die Angabe des Schemas gewährleistet die typsichere Verarbeitung der Nachricht.

Beispiel:

```
...
<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/final/types
    http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd">
  ...
</ReqMsg>
...
```

II.6.4 Integration von FinTS-Transaktionen in Fremdformate

Die Integration von FinTS-Geschäftsvorfällen in Fremdformate geschieht analog zu *II.6.3 Integration von FinTS-Nachrichten in Fremdformate*. Der Unterschied besteht lediglich darin, dass für die FinTS-Transaktionen ein zusätzliches Namensraum-Präfix deklariert werden sollte, um die Lesbarkeit zu erhöhen.

Beispiel:

```
...
<fintstrans:SingRemitt_1_Req
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
  schemaLocation="http://www.fints.org/spec/xmlschema/4.0/
    http://www.fints.org/spec/xmlschema/4.0/final/transactions/SingRemitt-4.xsd">
  ...
</fintstrans:SingRemitt_1_Req>
...
```

| | | | | |
|----------|----|------------|-------------------------|--|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 26 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax |
| | | Abschnitt: | FinTS-Datentypen | |

II.7 FinTS-Datentypen

Die FinTS-Datentypen sind konform zur XML Schema Spezifikation des W3C modelliert. Der Abschnitt vermittelt die wichtigsten Modellierungsprinzipien für XML-Schemas, die in FinTS angewendet werden. Leser, die mit der Modellierung von XML-Schemas vertraut sind, können diesen Abschnitt überspringen.

II.7.1 Binäre Daten

Binäre Daten werden durch den FinTS-Datentyp *bin* modelliert, der vom XML-Schema-Datentyp *base64Binary* abgeleitet wird. Es gelten dieselben Kodierungsregeln wie für den *base64Binary*-Datentyp gemäß [XML Schema 2].

II.7.2 Transparente Daten

Transparente Daten (siehe [Formals], Abschnitt *II.2 Syntaktische Festlegungen*) werden als binäre Daten eingestellt (siehe *II.7.1 Binäre Daten*).

II.7.3 Status und Anzahl

Status und Anzahl eines Elements werden in XML-Schema durch die Facetten *minOccurs* und *maxOccurs* für minimale und maximale Anzahl modelliert. Eine Muss-Datenstruktur erhält in der Schemabeschreibung den Wert *1* für *minOccurs*, eine optionale Datenstruktur erhält den Wert *0*. Die maximale Anzahl für das Auftreten einer Datenstruktur wird durch den Wert der Facette *maxOccurs* bestimmt. Der Wert *unbounded* definiert eine unbeschränkte Häufigkeit für das Auftreten einer Datenstruktur.

Für die Facetten in XML Schema existieren Standard-Belegungen, so dass in einem Schema nicht alle Facetten definiert sein müssen. Die Facette *minOccurs* ist mit dem Vorgabewert *1* belegt. Deshalb handelt es sich um eine Muss-Datenstruktur, falls sie nicht explizit mit einem Wert belegt ist. Auch die Facette *maxOccurs* ist mit dem Standardwert *1* belegt (s. Beispiel).

Im Beispiel wird festgelegt, dass das Element *PublicKey* bis zu zweimal auftreten oder entfallen kann.

```
<xs:element name="PublicKey" minOccurs="0" maxOccurs="2">
  ...
</xs:element>
```

II.7.4 Längenangaben

Die Facetten *length* bzw. *minLength* und *maxLength* legen im XML-Schema die Länge eines einfachen (unstrukturierten) Typs (simple type) fest. Für die in FinTS verwendeten einfachen Typen *string* und *binary* existieren Facetten, welche die Länge eines Typs beschreiben. Für Datums-Typen und numerische Typen hingegen nicht.

Die minimale und maximale Länge eines Typs werden in XML Schema durch die Facetten *minLength* und *maxLength* beschrieben. Die Facette *maxLength* wird zur Definition einer variablen Länge mit einer Längenbegrenzung im Schema mit dem Wert der Länge des Feldes belegt. Bei einer fest vorgeschriebenen Feldlänge wird die Facette *length* belegt.

Beispiel für eine fest vorgeschriebene Feldlänge:

```
<xs:element name="CountryCode" length="3"/>
```

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: FinTS-Datentypen | Stand: 09.07.2004 | Seite: 27 |

II.7.5 Aufzählungstypen

Aufzählungstypen werden in FinTS durch die Ableitung von einem einfachen FinTS-Datentyp beschrieben. Dabei wird der Wertebereich des abgeleiteten Typs durch eine Liste von Aufzählungswerten eingeschränkt.

Im Beispiel wird die *Rolle des Signierenden* durch drei Aufzählungswerte beschrieben. Der Typ der Aufzählungswerte ist durch Einschränkung vom Typ *an* (alphanumerisch) abgeleitet.

```
<xs:element name="SignerRole">
  <xs:simpleType>
    <xs:restriction base="an">
      <xs:enumeration value="ISS"/>
      <xs:enumeration value="WIT"/>
      <xs:enumeration value="MSG"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
```

| | | | | |
|----------|----|----------|------------|---|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | | | Dokument: XML-Syntax |
| Seite: | 28 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax |
| | | | | Abschnitt: Referenzierung mit XPath-Ausdrücken |

II.8 Referenzierung mit XPath-Ausdrücken

In FinTS-Nachrichten können Elemente durch [XPath]-Ausdrücke referenziert werden. Die Referenzierung von Elementen innerhalb einer Nachricht wird in verschiedenen Kontexten angewendet: Bei den Rückmeldungen zu Benutzernachrichten, bei der Signierung und als Kennzeichnung des Überbringers eines Nachrichtenteils. In FinTS sind nur bestimmte Formen der Referenzierung zulässig, die weiter unten in diesem Abschnitt beschrieben werden.

Die Vorschriften zur Bildung eines XPath-Ausdrucks werden bei der Beschreibung der jeweiligen Verwendung (z.B. im Abschnitt *IV.3 Botensignatur*) anhand der folgenden Attribute festgelegt:

Referenz-Ziel(e)

Es wird festgelegt, auf welche Elemente referenziert werden darf bzw. welche zwingend referenziert werden müssen.

Gültigkeitsbereich

Der Gültigkeitsbereich gibt das Wurzelement *R* desjenigen Teilbaums an, innerhalb dessen der Ausdruck gültig sein muss. Dieses bedeutet, dass das Ergebnis eines jeden Lokalisierungsschrittes innerhalb eines Lokalisierungspfades ein Element der Knotenmenge *M*, gebildet aus *R* sowie allen seinen Nachfolgern, sein muss.

Kontext

Optional wird der Kontext zur Auswertung des XPath-Ausdrucks angegeben. Die Angabe kann entfallen, wenn der Kontext durch den äußeren Rahmen vorgegeben ist (z. B. Verwendung in [XPath Filter]).

Zulässiger Ausdruck

Es wird festgelegt, welche der unten beschriebenen Lokalisierungspfade für die Angabe in einem XPath-Element erlaubt sind.

Zur Referenzierung wird eine eingeschränkte Form der abgekürzten Syntax gemäß [XPath] verwendet. Die Referenzierungsausdrücke müssen - soweit nicht anders angegeben - einem der folgenden Ausdrücke für Lokalisierungspfade genügen.

Absoluter Lokalisierungspfad:

```
AbsoluteLocationPath ::= '/' RelativeLocationPath?
```

Relativer Lokalisierungspfad:

```
RelativeLocationPath ::= Step ( '/' Step )*
```

Relativer Lokalisierungspfad für Verwendung in [XPath Filter]-Ausdrücken:

```
HereLocationPath ::= ('here()/' RelativeLocationPath)
```

mit:

```
Step ::= ( QName Predicate? )
       | '..'
QName ::= Prefix ':' LocalName
LocalName ::= NCName
Predicate ::= '[' Index ']'
Index ::= [1-9] ([0-9])*
```

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: II |
| Kapitel: Nachrichtensyntax Abschnitt: Referenzierung mit XPath-Ausdrücken | Stand: 09.07.2004 | Seite: 29 |

Es gelten die Hinweise zur formalen Grammatik aus *II.4 Verbandseigene Geschäftsvorfälle*.

♦ Erläuterungen:

Ein Lokalisierungsschritt (*Step*) besteht aus einem Knotentest mit qualifiziertem Elementnamen sowie einem Prädikat für den Index des Knotens. Der Lokalisierungsschritt *prefix:localName[i]* verweist somit auf das i-te Kindelement des Kontextknotens mit dem Namen *localName* und dem durch *prefix* definierten Namensraum.

Der Lokalisierungsschritt „.“ verweist auf das Elternelement des Kontextknotens.

Ein relativer Lokalisierungspfad (*RelativeLocationPath*) wird aus einer Folge von einem oder mehreren Lokalisierungsschritten gebildet, welche durch das Zeichen / getrennt und von links nach rechts interpretiert werden. Jeder Schritt verweist auf genau einen Elementknoten, welcher den Kontextknoten für den nächsten Schritt darstellt. Der Kontextknoten für den ersten Schritt ist das Elternelement des Textknotens, welcher den XPath-Ausdruck enthält.

Ein absoluter Lokalisierungspfad (*AbsoluteLocationPath*) wird von dem Zeichen / angeführt, welches den Kontextknoten für den ersten Lokalisierungsschritt auf den Wurzelknoten des Dokuments setzt, das den Knoten mit dem XPath-Ausdruck enthält.

Hinweis:

Der Wurzelknoten des Dokuments ist nicht zu verwechseln mit dem Elementknoten des Dokumentenelements, welches seinerseits ein Kind des Wurzelknotens darstellt (siehe auch [XPath], Abschnitt Datenmodell).

Die Funktion *here()* ist eine Erweiterung zum [XPath]-Standard gemäß [XPath Filter]. Sie setzt den Kontextknoten für den ersten Lokalisierungsschritt eines Lokalisierungspfades innerhalb einer [XPath Filter]-Transformation auf den Elternknoten des Textknotens, welcher den XPath-Ausdruck enthält und ermöglicht somit die Bildung von Lokalisierungspfaden relativ zu diesem Kontextknoten (*HereLocationPath*). Ohne Verwendung der *here()*-Funktion ist der Kontextknoten einer [XPath Filter]-Transformation der Wurzelknoten des Dokuments, welches die Eingabeknotenmenge der Transformation enthält.

Bei der Verwendung in [XPath Filter] ist insbesondere die Vereinigung von Lokalisierungspfaden mittels des Vereinigungsoperators | erlaubt. Die resultierende Knotenmenge nach der [XPath-Filter]-Transformation ist die Vereinigung der resultierenden Knotenmengen der einzelnen Lokalisierungspfade in Dokumentordnung.

Das Namensraumpräfix muss gemäß [Namespaces] in dem Element deklariert werden, welches den XPath-Ausdruck enthält, oder in einem dazu übergeordneten Element.

| | | | | |
|----------|----|----------|------------|---|
| Kapitel: | II | Version: | 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: | 30 | Stand: | 09.07.2004 | Kapitel: Nachrichtensyntax Abschnitt: Referenzierung mit XPath-Ausdrücken |

Beispiel:

Das Element *BankCode* aus einer Benutzernachricht, enthielt eine falsche Kennung. Deshalb enthält die Kreditinstitutsnachricht im Element *ElementRef* eine Referenz auf den ungültigen Eintrag.

```

...
<MsgRespState xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <RespCode>9210</RespCode>
  <ElementRef
    xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types">
/fintstype:ReqMsg[1]/fintstype:ReqMsgHeader[1]/fintstype:BankID[1]/fintstype:BankCode
[1]</ElementRef>
    <RespText>Kennung nicht erlaubt.</RespText>
  </MsgRespState>
...

```

II.9 Symbole in den Schemadiagrammen

Die nächsten Kapitel beschreiben die Schemas zum Aufbau von FinTS-Nachrichten in der Form von Diagrammen. In den beiden folgenden Beispielen werden die in den Diagrammen verwendeten Symbole beschrieben.

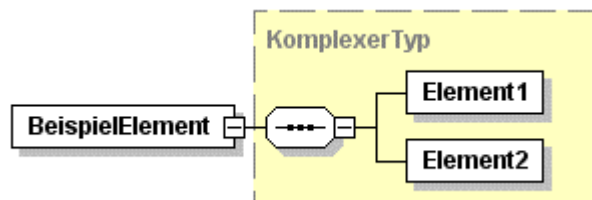


Abbildung 1: Beispiel für eine Elementdeklaration

In den Diagrammen zu den FinTS-Schemas werden Elemente durch eine Textbox abgebildet, die den Elementnamen enthält. Das deklarierte Element befindet sich auf der linken Seite des Diagramms. Zu jedem Element gehört eine hierarchische Typbeschreibung (Inhaltsmodell), die sich rechts vom Element befindet. Wenn zur Beschreibung des Inhaltsmodells auf einen vordefinierten Typ referenziert wird, ist dieser Typ von einem gestrichelten Rahmen umgeben. Wenn kein vordefinierter Typ verwendet wird, handelt es sich um eine namenlose (anonyme) Typdefinition.

Im Beispiel wird das Inhaltsmodell des Elements *BeispielElement* durch eine Sequenz von zwei Elementen (*Element1* und *Element2*) definiert. Die Definition des Inhaltsmodells erfolgt durch die Verwendung des Typs *complexType*.

Bei einer Typdefinition wird das Inhaltsmodell auf dieselbe Weise abgebildet wie bei einer Elementdeklaration. Zur Unterscheidung wird der Typ durch eine Textbox mit abgerundeten Ecken dargestellt.

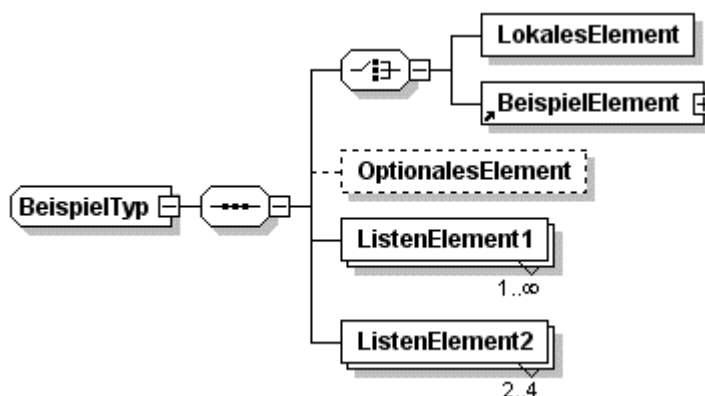


Abbildung 2: Beispiel für eine Typdefinition

Die Inhaltsmodelle der definierten Typen enthalten Sequenzen und Wahlmöglichkeiten. Bei einer Sequenz enthält das übergeordnete Element (auf der linken Seite des Sequenzsymbols) die untergeordneten Elemente (auf der rechten Seite des Sequenzsymbols) in der im Diagramm von oben nach unten festgelegten Reihenfolge. Bei einer Wahlmöglichkeit enthält das übergeordnete Element genau eines der sich unter dem Schaltersymbol befindlichen Elemente.

Optionale Teile des Inhaltsmodells werden durch gestrichelte Linien und Textboxen repräsentiert. Wenn Komponenten des Inhaltsmodells häufiger als einmal auftreten können, wird an den zugehörigen Symbolen der Häufigkeitsbereich annotiert. Der

| | | |
|----------------|----------------------|---|
| Kapitel: II | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 32 | Stand: 09.07.2004 | Kapitel: Nachrichtensyntax Abschnitt: Symbole in den Schemadiagrammen |

Häufigkeitsbereit $1..∞$ für ein Element gibt an, dass dieses Element einmal oder beliebig oft nacheinander auftreten kann.

Im vorangehenden Beispiel besteht das Inhaltsmodell des Typs *BeispielTyp* aus der Sequenz „Wahlmöglichkeit zwischen *LokalesElement* und *BeispielElement*“, *OptionalesElement*, *ListenElement1* und *ListenElement2*. Der Typ von *LokalesElement* wird in der Typdefinition von *BeispielTyp* festgelegt. Das Element *BeispielElement* wird durch die Referenz auf eine globale Elementdeklaration beschrieben. Eine solche Referenz wird durch einen schrägen Pfeil symbolisiert. Das in der Sequenz nach der Wahlmöglichkeit positionierte Element *OptionalesElement* kann einmal auftreten oder entfallen. Das Element *ListenElement1* tritt mindestens einmal und beliebig oft auf. Das Element *ListenElement2* wird aufeinander folgend 2 bis 4-mal verwendet.

| | | |
|--|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Symbole in den Schemadiagrammen | Stand: 09.07.2004 | Seite: 33 |

III. NACHRICHTENAUFBAU

| | |
|---|-----------|
| III.1 Überblick..... | 35 |
| III.2 Allgemeiner Aufbau von Benutzernachricht und Kreditinstitutsnachricht..... | 37 |
| III.2.1 Benutzernachricht..... | 37 |
| III.2.1.1 Nachrichtenkopf einer Benutzernachricht | 37 |
| III.2.1.2 Nachrichtenkörper einer Benutzernachricht..... | 38 |
| III.2.1.3 Initialisierung | 39 |
| III.2.1.4 Auftrag | 41 |
| III.2.2 Kreditinstitutsnachricht | 41 |
| III.2.2.1 Nachrichtenkopf einer Kreditinstitutsnachricht | 42 |
| III.2.2.2 Nachrichtenkörper einer Kreditinstitutsnachricht..... | 42 |
| III.2.2.3 Initialisierungsantwort..... | 44 |
| III.2.2.4 Gesamtrückmeldung zur Nachricht..... | 45 |
| III.2.2.5 Rückmeldungen zur Nachricht | 45 |
| III.2.2.6 Gesamtrückmeldung zum Auftragsteil | 46 |
| III.2.2.7 Rückmeldungen zum Auftragsteil..... | 46 |
| III.2.2.8 Auftragsantwort | 47 |
| III.3 Verschiedene Benutzer- und Antwortnachrichten..... | 49 |
| III.3.1 Standard-Nachricht..... | 49 |
| III.3.2 Anonyme Nachricht | 50 |
| III.3.3 Lebendmeldung..... | 52 |
| III.3.4 Synchronisierung..... | 54 |
| III.4 Keymanagement-Nachrichten | 56 |
| III.4.1 Anforderung der Kreditinstitutsschlüssel | 56 |
| III.4.2 Erstmalige Übermittlung eines Kundenschlüssels..... | 59 |
| III.4.3 Schlüsseländerung | 62 |
| III.4.4 Schlüsselsperrung | 65 |
| III.5 Bankparameterdaten | 69 |
| III.6 User-Parameterdaten..... | 76 |
| III.7 Administrative Aufträge | 79 |
| III.7.1 BPD | 79 |
| III.7.1.1 BPD anfordern..... | 79 |
| III.7.2 UPD | 80 |
| III.7.2.1 UPD anfordern..... | 80 |
| III.7.3 Intermediärszenarien | 82 |
| III.7.3.1 Liste der Intermediäre..... | 82 |
| III.7.3.2 Für einen Intermediär anmelden | 83 |
| III.7.3.3 Für einen Intermediär abmelden | 83 |

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 34 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Symbole in den Schemadiagrammen |

| | | |
|-----------|--|-----|
| III.7.3.4 | UPDI ändern | 84 |
| III.7.4 | PIN/TAN | 85 |
| III.7.4.1 | PIN ändern..... | 85 |
| III.7.4.2 | TAN-Liste anfordern | 86 |
| III.7.4.3 | TAN-Liste freischalten | 86 |
| III.7.4.4 | PIN sperren | 87 |
| III.7.4.5 | PIN-Sperre aufheben..... | 88 |
| III.7.4.6 | TAN-Liste sperren/löschen..... | 88 |
| III.7.4.7 | TAN-Verbrauchsinformationen anfordern | 89 |
| III.7.5 | Abonnement | 90 |
| III.7.5.1 | Abonnement einreichen..... | 90 |
| III.7.5.2 | Abonnement löschen..... | 93 |
| III.7.5.3 | Abonnementsinformationen anfordern | 94 |
| III.7.6 | Adressenregistrierung | 95 |
| III.7.6.1 | Adresse registrieren | 95 |
| III.7.6.2 | Adressregistrierungsinformationen holen..... | 96 |
| III.7.6.3 | Adressregistrierung löschen..... | 97 |
| III.7.7 | Quittung | 98 |
| III.7.7.1 | Quittung | 98 |
| III.7.8 | Verteile Signaturen | 99 |
| III.7.8.1 | Auftrag mit verteilten Signaturen einreichen | 99 |
| III.7.8.2 | Informationen zu Auftrag mit verteilten Signaturen | 100 |
| III.7.8.3 | Auftrag mit verteilten Signaturen signieren | 102 |
| III.7.8.4 | Auftrag mit verteilten Signaturen löschen..... | 102 |
| III.7.9 | Statusprotokoll..... | 103 |
| III.7.9.1 | Statusprotokoll..... | 103 |

III.1 Überblick

Die folgenden Abbildungen geben einen Überblick über den Nachrichtenaufbau in FinTS. Eine FinTS-Nachricht ist entweder eine Benutzer- oder eine Kreditinstitutsnachricht. Beide Nachrichtenformen folgen demselben prinzipiellen Aufbau.

Sie sind in einen Nachrichtenkopf (Header) und einen Nachrichtenkörper (Body) unterteilt. Der Nachrichtenkörper enthält genau einen von acht möglichen Nachrichtentypen. Der Aufbau dieser Nachrichtentypen wird in den folgenden Abschnitten genauer beschrieben.

Die generelle Verwendung der Nachrichten im FinTS-Protokoll ist in den anderen Teilen der Spezifikation ([Formals], [HBCI], [PINTAN]) beschrieben. Die Belegung einzelner Datenelemente kann außerdem im [DataDictionary] nachgesehen werden, das Dictionary ist nach den deutschsprachigen Begriffen sortiert, die in den Abbildungen jeweils als Anmerkung an den Elementen angebracht sind. Spezielle Belegungsvorschriften im besonderen Kontext eines Nachrichtentyps sind bei der jeweiligen Nachrichtenbeschreibung angegeben.

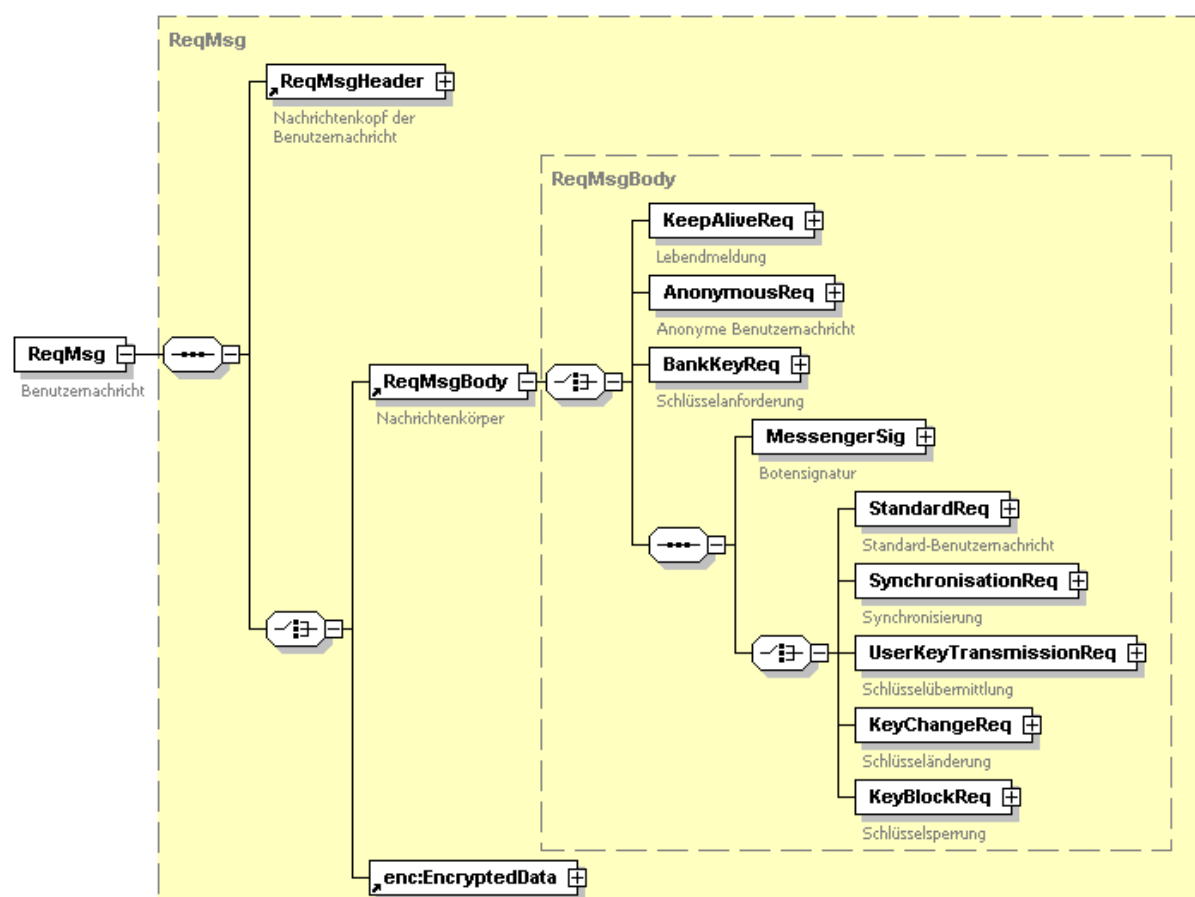


Abbildung 3: Benutzernachricht

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 36 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Überblick |

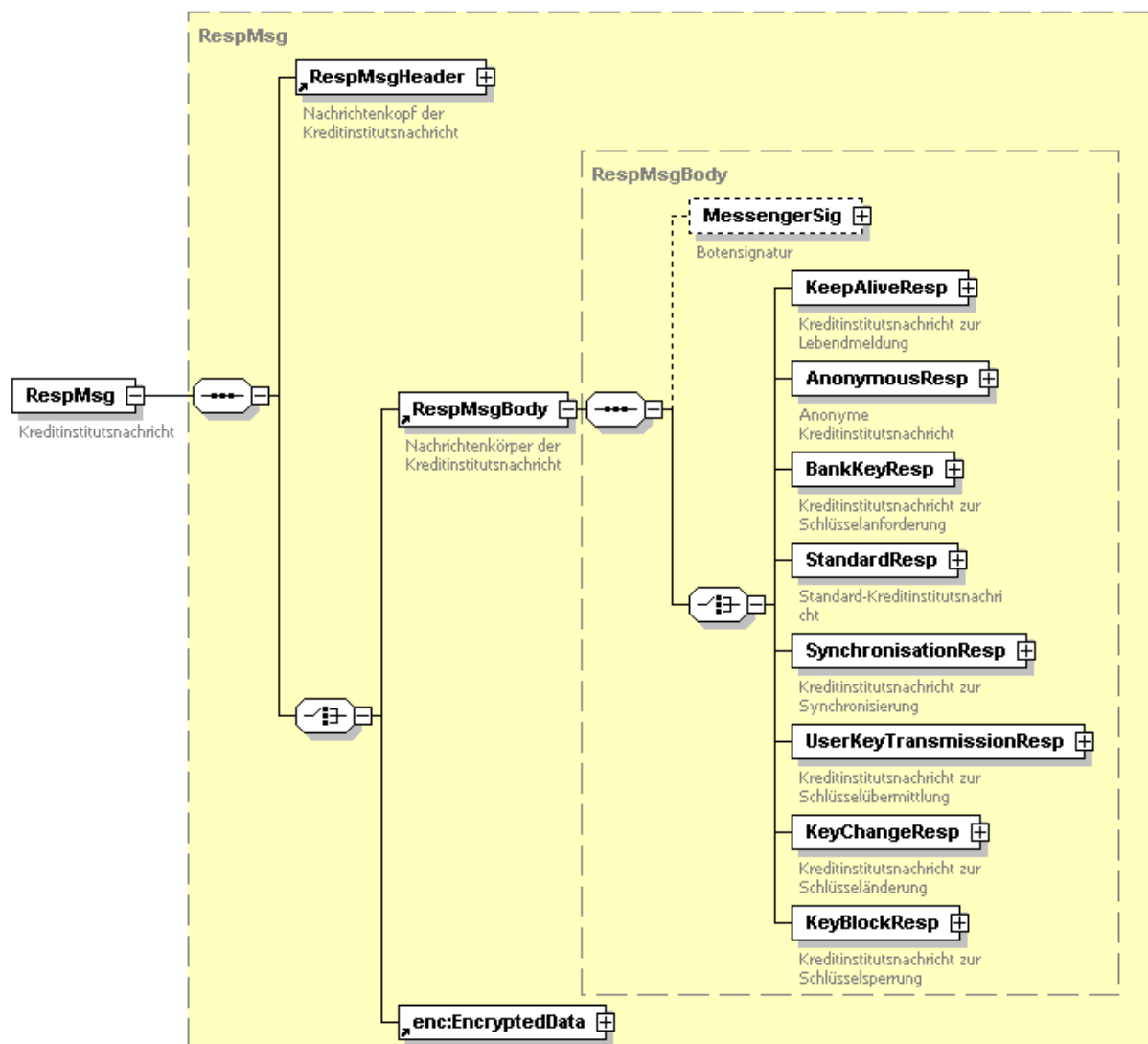


Abbildung 4: Kreditinstitutsnachricht

| | | |
|---|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und | Stand: 09.07.2004 | Seite: 37 |

III.2 Allgemeiner Aufbau von Benutzernachricht und Kreditinstitutsnachricht

Dieser Abschnitt erläutert den grundsätzlichen Aufbau der Nachrichten. Die Besonderheiten der acht unterschiedlichen Nachrichtentypen werden in den Abschnitten *III.3 Verschiedene Benutzer- und Antwortnachrichten* und *III.4 Keymanagement-Nachrichten* näher beleuchtet. Zum Nachrichtenaufbau siehe auch [Formals], Abschnitt *II.9 Benutzernachrichten allgemein* und [Formals], Abschnitt *II.10 Kreditinstitutsnachrichten allgemein*.

III.2.1 Benutzernachricht

Eine Benutzernachricht besteht aus dem Nachrichtenkopf (*ReqMsgHeader*) und dem Nachrichtenkörper (*ReqMsgBody*) (siehe auch Abbildung 3).

Der Nachrichtenkörper kann verschlüsselt (als *enc:EncryptedData*) oder unverschlüsselt (als *ReqMsgBody*) übertragen werden.

Bei der verschlüsselten Übertragung ersetzt das *EncryptedData*-Element das Element *ReqMsgBody*. Dabei wird der Nachrichtenkörper durch den [XML Encryption]-Standard verschlüsselt. Bei der Verschlüsselung des Nachrichtenkörpers befindet sich der verschlüsselte Inhalt von *ReqMsgBody* innerhalb des *EncryptedData*-Elements (siehe *V.2 Verschlüsselung des Nachrichtenkörpers*). In welchen Fällen der Nachrichtenkörper verschlüsselt werden muss, ist in [Formals], Abschnitt *II.13 Verschlüsselung der Kommunikation* festgelegt. Zusätzlich oder statt der Verschlüsselung kann auf formal gleiche Art eine Komprimierung des Nachrichtenkörpers stattfinden, siehe [Formals], Abschnitt *II.14 Komprimierung* und *V.4 Komprimierung*.

Der Inhalt des Nachrichtenkörpers sowie des Nachrichtenkopfes wird bei den meisten Nachrichtentypen mit einer Botensignatur im Element *MessengerSig* versehen. Die Botensignatur wird im Abschnitt *IV.3 Botensignatur* beschrieben. Festlegungen zur Verwendung der Signaturen in FinTS finden sich in [Formals], Abschnitt *II.12.4 Vorgehensweise beim Signieren und Verschlüsseln* und [Formals], Abschnitt *II.4 Signatur-Rollenverteilung bei Kommunikation mit und ohne Intermediär*.

Signierte (personalisierte) Nachrichtentypen sind die Standard-Benutzernachricht (*StandardReq*), die Synchronisierung (*SynchronisationReq*), die erstmalige Übermittlung eines Kundenschlüssels (*UserKeyTransmissionReq*), die Schlüsseländerung (*KeyChangeReq*), sowie die Schlüsselsperrung (*KeyBlockReq*).

Unsignierte (anonyme) Nachrichtentypen sind die anonyme Benutzernachricht (*AnonymousReq*), die Lebendmeldung (*KeepAliveReq*), sowie die Anforderung eines Bank-Schlüssels (*BankKeyReq*).

III.2.1.1 Nachrichtenkopf einer Benutzernachricht

Der Nachrichtenkopf der Benutzernachricht enthält die Identifizierung des Kreditinstituts (*BankID*), eine Nachrichtennummer (*MsgNo*) und die Benutzer- und Kreditinstitutsseitigen Referenzen (*UserRef*, *UserTextRef* bzw. *BankRef*) zur Steuerung des Dialogablaufs (siehe dazu auch [Formals], Abschnitt *II.6 Synchrone Kommunikationsverfahren*). Er liegt außerhalb des verschlüsselbaren Teilbaums, wird aber von der Botensignatur signiert.

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 38 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

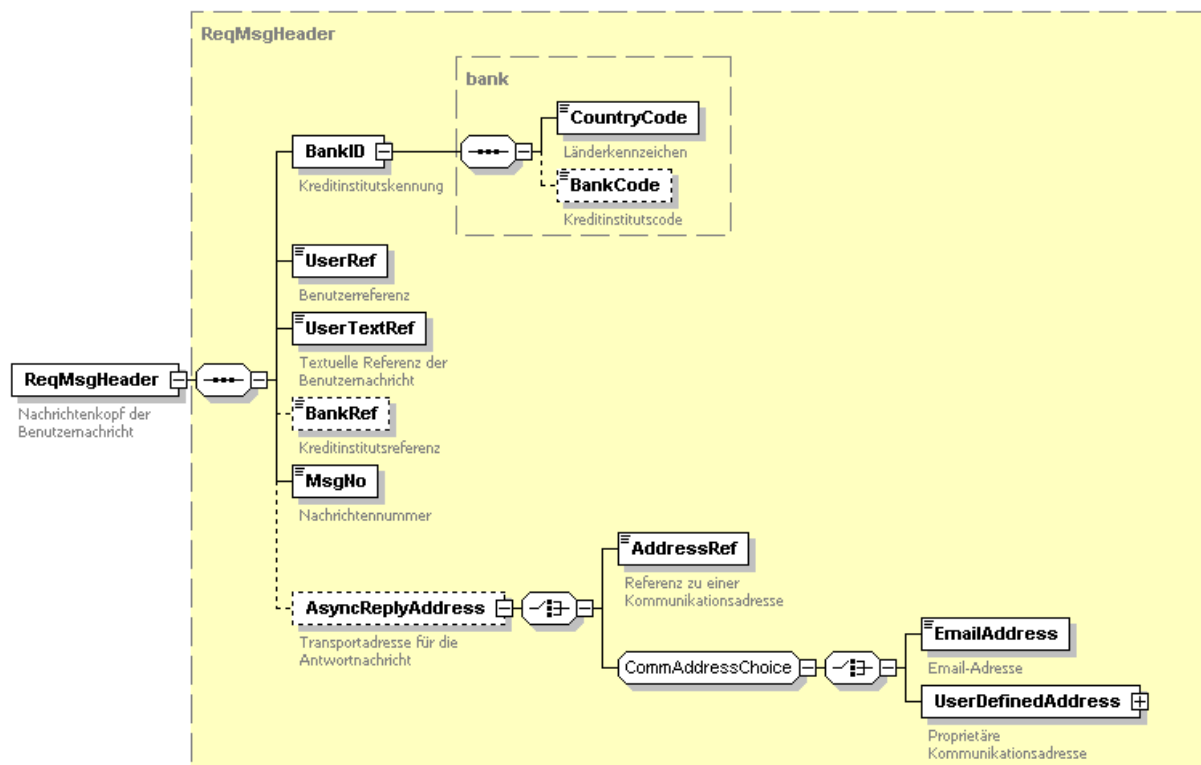


Abbildung 5: Nachrichtenkopf einer Benutzernachricht

Für asynchrone Kommunikationsverfahren (siehe [Formals], Abschnitt II.7 *Asynchrone Kommunikationsverfahren (Datagramme)*) ist die Angabe einer Antwort-Email-Adresse (**AsyncReplyAddress**) möglich.

III.2.1.2 Nachrichtenkörper einer Benutzernachricht

Alle Nachrichtentypen außer dem der Lebendmeldung enthalten einen oder mehrere Auftragsteile (*RequestList*), in die unterhalb von *Orders* jeweils mehrere Aufträge eingestellt werden können (siehe [Formals], Abschnitt II.9 *Benutzernachrichten allgemein*). Auftragsteile können in gleicher Weise wie der Nachrichtenkörper verschlüsselt und/oder komprimiert werden (siehe V.3 *Verschlüsselung von Aufträgen und Auftragsantworten* und V.4 *Komprimierung*). Zum Einsatz der Auftragsverschlüsselung in FinTS siehe auch [Formals], Abschnitt II.12.2 *Teilverschlüsselte Nachrichten*.

| | | |
|---|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und | Stand: 09.07.2004 | Seite: 39 |

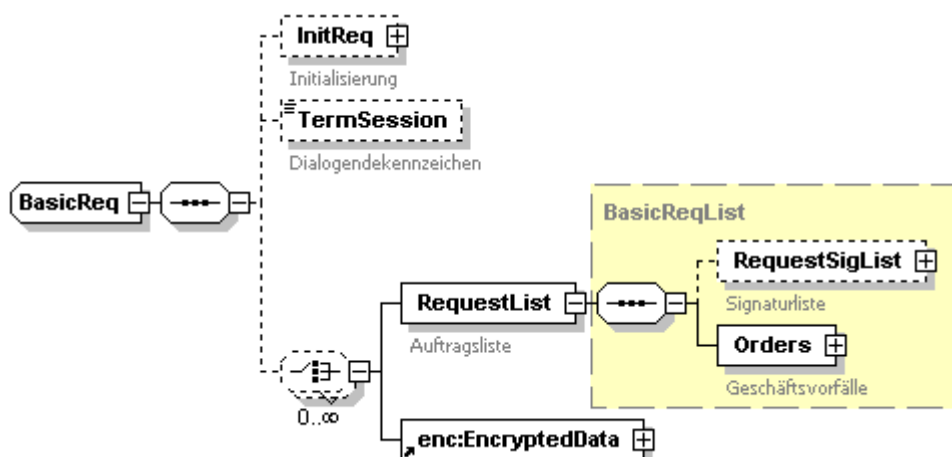


Abbildung 6: Basistyp für die Nachrichtenkörper der Benutzernachricht

In den personalisierten Nachrichtentypen kann ein Auftragsteil mit einer oder mehreren Auftragssignaturen in der *RequestSigList* versehen werden. Die Auftragssignatur wird im Abschnitt IV.4 *Auftragssignatur* beschrieben.

Alle Nachrichtentypen außer der Lebendmeldung enthalten eine Initialisierung (*InitReq*), die zur Einleitung eines Dialogs dient (siehe [Formals], Abschnitt II.6 *Synchrone Kommunikationsverfahren*). In einem Dialog mit Standard-Benutzernachrichten ist sie ausschließlich in der ersten Nachricht zu verwenden. Bei allen anderen Nachrichtentypen ist sie ein Pflichtfeld, dadurch kann eine solche Nachricht nicht als Folgenachricht einer Dialogfolge verwendet werden.

Mit dem Element *TermSession* wird angezeigt, dass ein Dialog mit dieser Nachricht endet (vgl. [Formals], Abschnitt II.6.2 *Dialogbeendigung und Endenachrichten*). Es muss in einem Dialog mit Standard-Benutzernachrichten genau in der letzten Benutzernachricht eingefügt werden, bei allen anderen Nachrichtentypen ist es zwingend vorhanden - damit kann einer solchen Nachricht keine weitere Nachricht eines Dialogs folgen.

Zusammen mit der zwingenden Initialisierung folgt daraus, dass alle Nachrichtentypen außer der Standard-Benutzernachricht und der Lebendmeldung ausschließlich als FinTS-Datagramme verwendet werden (vgl. [Formals], Abschnitt II.7 *Asynchrone Kommunikationsverfahren (Datagramme)*).

III.2.1.3 Initialisierung

Die Initialisierung zur Einleitung eines Dialogs besteht aus den Segmenten zur Identifikation (*Identification*) und zur Verarbeitungsvorbereitung (*ProcPreparation*), vgl. auch [Formals], Abschnitt II.15 *Initialisierung*.

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 40 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

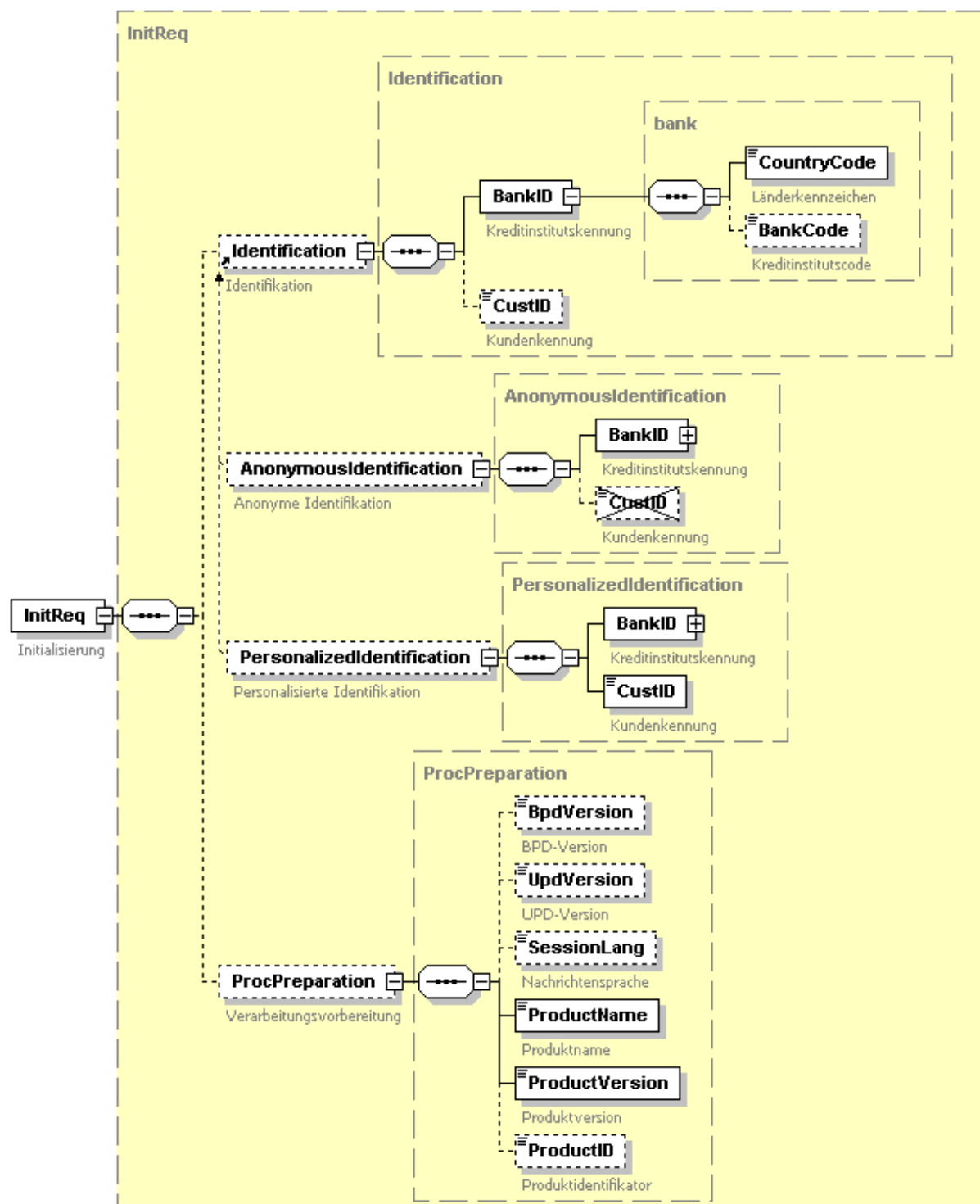


Abbildung 7: Initialisierung

Das Segment zur Identifikation existiert in einer anonymen Ausprägung (*AnonymousIdentification*) für die anonyme Benutzernachricht und einer personalisierten Ausprägung (*PersonalizedIdentification*) für die anderen (personalisierten) Nachrichtentypen. Sie unterscheiden sich nur darin, dass die personalisierte Variante zwingend eine Kundenkennung (*CustID*) enthält, die anonyme Variante hingegen keine Kundenkennung enthalten kann.

| | | |
|---|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und | Stand: 09.07.2004 | Seite: 41 |

III.2.1.4 Auftrag

Ein Auftrag ist in der Auftragsliste unterhalb des Elements *Orders* als freies Inhaltsmodell definiert. Hier wird in der Standard-Benutzernachricht ein beliebiger Geschäftsvorfall aus dem Namensraum für FinTS-Transaktionen oder einem individuellen Namensraum (vgl. *II.4 Verbandseigene Geschäftsvorfälle*) eingestellt.

- Die in der FinTS-Spezifikation definierten Transaktionsaufträge und Abholaufträge finden sich in [Messages].
- Abschnitt *III.7 Administrative Aufträge* enthält administrative Aufträge zur Verwendung in der Standard-Benutzernachricht.
- In anonymen Benutzernachrichten können nur bestimmte Geschäftsvorfälle verwendet werden (vgl. [Formals], Abschnitt *II.17 Anonymer Zugang*).
- Für die anderen Nachrichtentypen sind jeweils spezielle administrative Geschäftsvorfälle definiert, die nur zusammen mit diesem Nachrichtentyp verwendet werden können - siehe dazu *III.3 Verschiedene Benutzer- und Antwortnachrichten*, *III.4 Keymanagement-Nachrichten*.

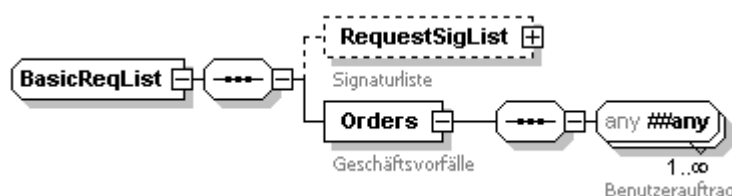


Abbildung 8: Benutzerauftrag im abstrakten Basistyp der Auftragsliste



Eine Auftragsliste stellt die kleinste syntaktische Einheit in einer Benutzernachricht dar, die FinTS-konform, unabhängig vom äußeren Kontext verarbeitbar ist.



III.2.2 Kreditinstitutsnachricht

Eine Kreditinstitutsnachricht hat denselben prinzipiellen Aufbau wie eine Benutzernachricht. Sie besteht aus einem Nachrichtenkopf (*RespMsgHeader*) und einem unverschlüsselten oder verschlüsselten Nachrichtenkörper (siehe Abbildung 4). Botensignatur, Verschlüsselung und Komprimierung sind analog zur Benutzernachricht modelliert, vgl. *III.2.1 Benutzernachricht*.

Den acht unterschiedlichen Typen der Benutzernachricht sind korrespondierende Typen der Kreditinstitutsnachricht zugeordnet.

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 42 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

III.2.2.1 Nachrichtenkopf einer Kreditinstitutsnachricht

Die folgende Abbildung zeigt den Aufbau eines Nachrichtenkopfs einer Kreditinstitutsnachricht.

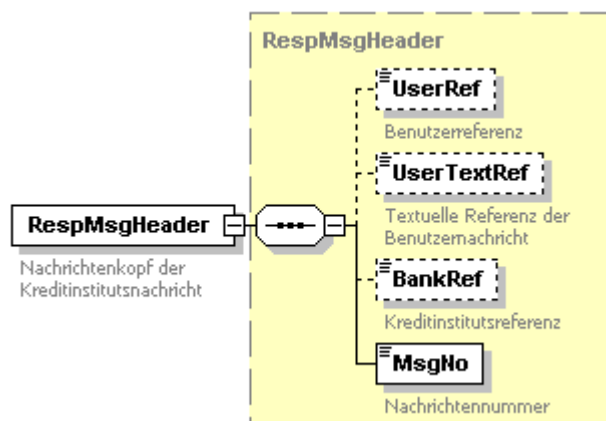


Abbildung 9: Nachrichtenkopf einer Kreditinstitutsnachricht

Im Nachrichtenkopf der Kreditinstitutsnachricht werden die Referenzen des Benutzers (*UserRef*, *UserTextRef*) und die Referenz des Kreditinstituts (*BankRef*) sowie die Nachrichtennummer der Benutzernachricht (*MsgNo*) zurück gemeldet (siehe dazu auch [Formals], Abschnitt II.15.2 *Kreditinstitutsnachricht*).

III.2.2.2 Nachrichtenkörper einer Kreditinstitutsnachricht

Der Nachrichtenkörper einer Kreditinstitutsnachricht ähnelt inhaltlich dem einer Benutzernachricht. Bei der Kreditinstitutsnachricht ist die Botensignatur allerdings für alle acht Nachrichtentypen optional. Die Inhaltsmodelle für die Nachrichtenkörper der verschiedenen Nachrichtentypen mit Ausnahme der Lebendmeldung sind von einem gemeinsamen Basistyp abgeleitet, Abbildung 10 zeigt diesen allgemeinen Aufbau.

| | | |
|---|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und | Stand: 09.07.2004 | Seite: 43 |

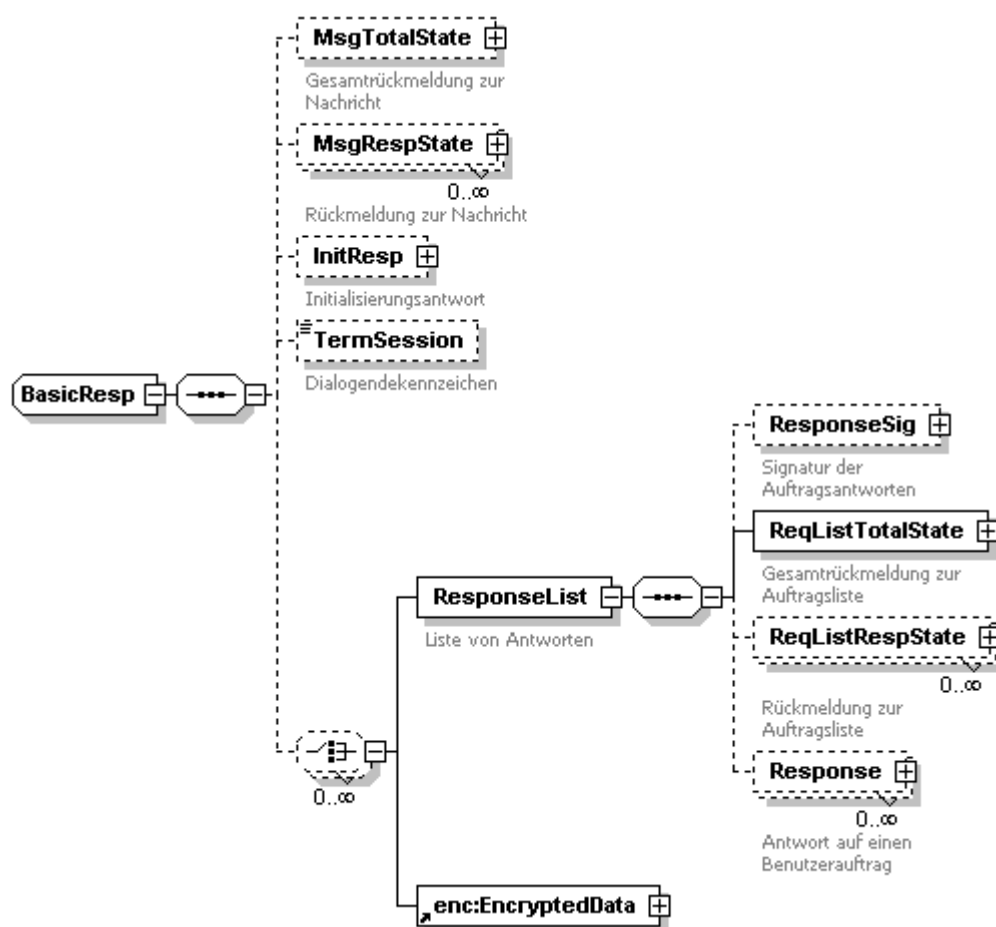


Abbildung 10: Basistyp für die Nachrichtenkörper der Kreditinstitutsnachricht

Die Nachrichten enthalten im Nachrichtenkörper beliebig viele Antwortlisten (*ResponseList*), die mit den Auftragslisten (*RequestList*) der Benutzernachricht korrespondieren und die Antworten zu den einzelnen Aufträgen transportieren. Verschlüsselung, Komprimierung und Signatur der Auftragsantworten sind analog zu III.2.1 *Benutzernachricht* modelliert.



Eine Antwortliste stellt die kleinste syntaktische Einheit in einer Kreditinstitutsnachricht dar, die [HBCI]-konform, unabhängig vom äußeren Kontext verarbeitbar ist.



Es ist wichtig, dass die Reihenfolge der Elemente *ResponseList* der Reihenfolge der korrespondierenden Elemente *RequestList* in der Benutzernachricht entspricht, damit dem Empfänger eine Zuordnung der Auftragsantworten möglich ist.



Die Initialisierung der Benutzernachricht wird in der Kreditinstitutsnachricht mit einer Initialisierungsantwort (*InitResp*) beantwortet, sofern zurück zu meldende Inhalte vorliegen.

Rückmeldungen zur Gesamtnachricht werden in den Elementen *MsgRespState* und *MsgTotalState* geliefert. Die Antwortlisten enthalten Rückmeldungen zu den Auftrags teilen sowie zu jedem Auftrag eine Antwort (*Response*).

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 44 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

Mit dem Element *TermSession* zeigt das Kreditinstitut analog zur Benutzernachricht das Ende eines synchronen Dialogs an. Das Kreditinstitut spiegelt dabei das Element *TermSession* aus der Benutzernachricht wieder. Davon abweichend wird das Element immer im Falle eines Dialogabbruches (siehe [Formals], Abschnitt II.16 *Dialogabbruchnachricht*) durch das Kreditinstitut gesetzt.

III.2.2.3 Initialisierungsantwort

Die Rückmeldung des Kreditinstituts auf die Initialisierung des Benutzers enthält

- aktuelle Bankparameterdaten, wenn der Benutzer keine oder eine veraltete Version gemeldet hat (*BankParamData*).
- aktuelle User-Parameterdaten, wenn der Benutzer keine oder eine veraltete Version gemeldet hat (*UserParamData*).
- im Sicherheitsverfahren HBCI, RDH-Variante, den - für das verwendete Sicherheitsprofil gültigen - aktuellen öffentlichen Verschlüsselungsschlüssel des Kreditinstituts (*PublicKey*), wenn der Benutzer in seiner Nachricht einen veralteten Schlüssel verwendet hat.
- Kreditinstitutsmeldungen (*BankMessage*) (freie Textinformationen des Instituts)

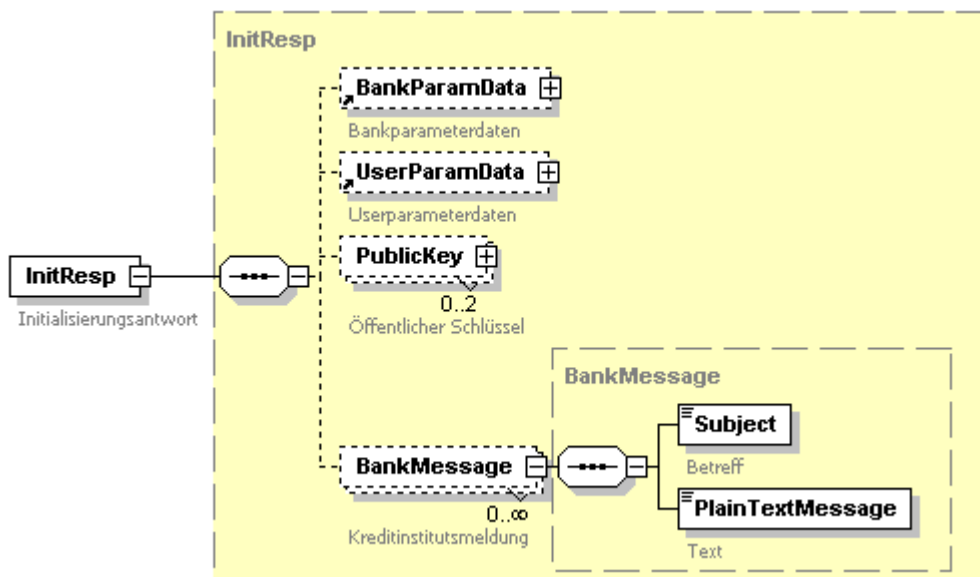


Abbildung 11: Initialisierungsantwort

III.2.2.4 Gesamtrückmeldung zur Nachricht

Das Element *MsgTotalState* enthält die Gesamtrückmeldung zur Nachricht (siehe auch [Formals], Abschnitt II.10.1 Rückmeldungen zur Nachricht). Es besitzt das Inhaltsmodell des Typs *TotalState*:

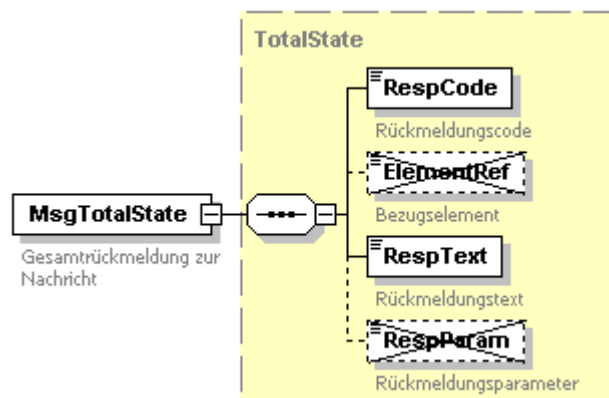


Abbildung 12: Gesamtrückmeldung zur Nachricht

RespCode und *RespText* enthalten den Status der Nachricht.

III.2.2.5 Rückmeldungen zur Nachricht

Das Element *MsgRespState* enthält eine Rückmeldung zur Nachricht (siehe auch [Formals], Abschnitt II.10.1 Rückmeldungen zur Nachricht). Es besitzt das Inhaltsmodell des Typs *ResponseState*:

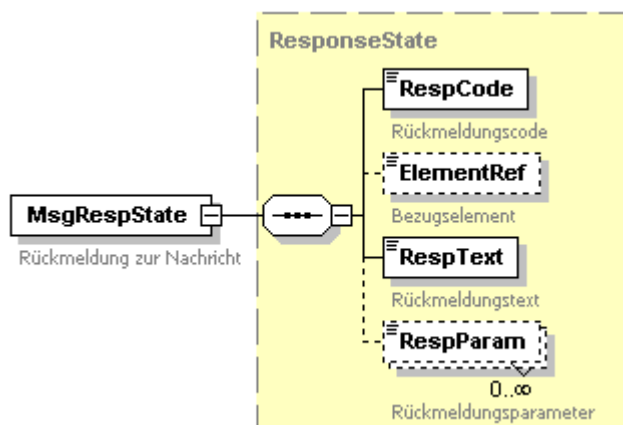


Abbildung 13: Rückmeldung zur Nachricht

RespCode und *RespText* enthalten eine Fehlerbeschreibung. In den *RespParam*-Elementen können zusätzliche Erläuterungen zu dieser Beschreibung aufgeführt werden (vgl. [Formals], Abschnitt II.11 Rückmeldungs-codes).

Durch die Angabe eines XPath-Ausdrucks im Element *ElementRef* kann in der Kreditinstitutsnachricht ein exakter Bezugspunkt in einer Benutzernachricht referenziert werden. Diese Referenz ist bei Elementrückmeldungen zu befüllen, nicht aber bei Meldungen zur Gesamtnachricht (siehe dazu [Formals], Abschnitt II.10.1 Rückmeldungen zur Nachricht).

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 46 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

Neben den Festlegungen in Abschnitt *II.8 Referenzierung mit XPath-Ausdrücken* gilt für die Belegung des Elements *ElementRef*:

| | |
|---------------------|---|
| Referenz-Ziel | Ein Element der Benutzernachricht, auf die sich die Kreditinstitutsnachricht bezieht. |
| Gültigkeitsbereich | Dokumentelement der Benutzernachricht, auf die sich die Kreditinstitutsnachricht bezieht. |
| Kontext | Der Kontext zur Auswertung des Lokalisierungspfades ist der Wurzelknoten der Benutzernachricht, auf die sich die Kreditinstitutsnachricht bezieht. |
| Zulässiger Ausdruck | Der Ausdruck im Element <i>ElementRef</i> muss der Bildungsregel für <i>LocationPath</i> genügen: $\text{LocationPath} ::= \text{AbsoluteLocationPath} \\ ::= \text{RelativeLocationPath}$ |

Beispiel:

```
<MsgRespState>
  xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types"
  <RespCode>9110</RespCode>

  <ElementRef>/fintstype:ReqMsg[1]/fintstype:ReqMsgHeader[1]/fintstype:BankID[1]</ElementRef>
  <RespText>Unbekannter Aufbau</RespText>
</MsgRespState>
```

III.2.2.6 Gesamtrückmeldung zum Auftragsteil

Das Element *ReqListTotalState* enthält die Gesamtrückmeldung zur Auftragsliste (siehe auch [Formals], Abschnitt *II.10.2 Rückmeldungen zum Auftragsteil*). Es ist wie *MsgTotalState* nach dem Inhaltsmodell des Typs *TotalState* aufgebaut.

III.2.2.7 Rückmeldungen zum Auftragsteil

Das Element *ReqListRespState* enthält eine Rückmeldung zum Auftragsteil. Es ist nach dem in *III.2.2.5 Rückmeldungen zur Nachricht* beschriebenen Inhaltsmodell *ResponseState* aufgebaut.

Für die Verwendung dieser Rückmeldung und insbesondere die Element-Referenzierung mittels *ElementRef* siehe [Formals], Abschnitt *II.10.2 Rückmeldungen zum Auftragsteil*. Für *ElementRef* gelten darüber hinaus die Festlegungen in Abschnitt *II.8 Referenzierung mit XPath-Ausdrücken* sowie:

| | |
|---------------------|--|
| Referenz-Ziel | Ein Element der Benutzernachricht, auf die sich die Kreditinstitutsnachricht bezieht. |
| Gültigkeitsbereich | Wurzelement der RequestList, auf die sich die Rückmeldung bezieht. |
| Kontext | Wurzelement der RequestList, auf die sich die Rückmeldung bezieht. |
| Zulässiger Ausdruck | Der Ausdruck in <i>XPath</i> muss der Bildungsregel für <i>RelativeLocationPath</i> genügen. |

| | | |
|---|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und | Stand: 09.07.2004 | Seite: 47 |

Beispiel:

```
<ResponseList xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ReqListRespState>
    <RespCode>9050</RespCode>
    <RespText>Teilweise fehlerhaft</RespText>
  </ ReqListRespState >
  <ReqListRespState>
    <RespCode>9330</RespCode>
    <ElementRef>ds:Signature[1]</ElementRef>
    <RespText>Signatur gesperrt</RespText>
  </ ReqListRespState >
  <Response>
    ...
  </Response>
</ResponseList>
```

III.2.2.8 Auftragsantwort

Die Antwort zu einem Auftrag (*Response*) enthält in der Standard-Kreditinstitutsnachricht und in der anonymen Kreditinstitutsnachricht ein Element mit freiem Inhaltsmodell zur Aufnahme der Antwortdaten von Abholaufträgen. Für Geschäftsvorfälle, die solche Antwortdaten liefern, muss das Antwortelement im gleichen Schema modelliert sein und zum selben Namensraum gehören wie der Auftrag (vgl. [Messages] und *III.7 Administrative Aufträge*).

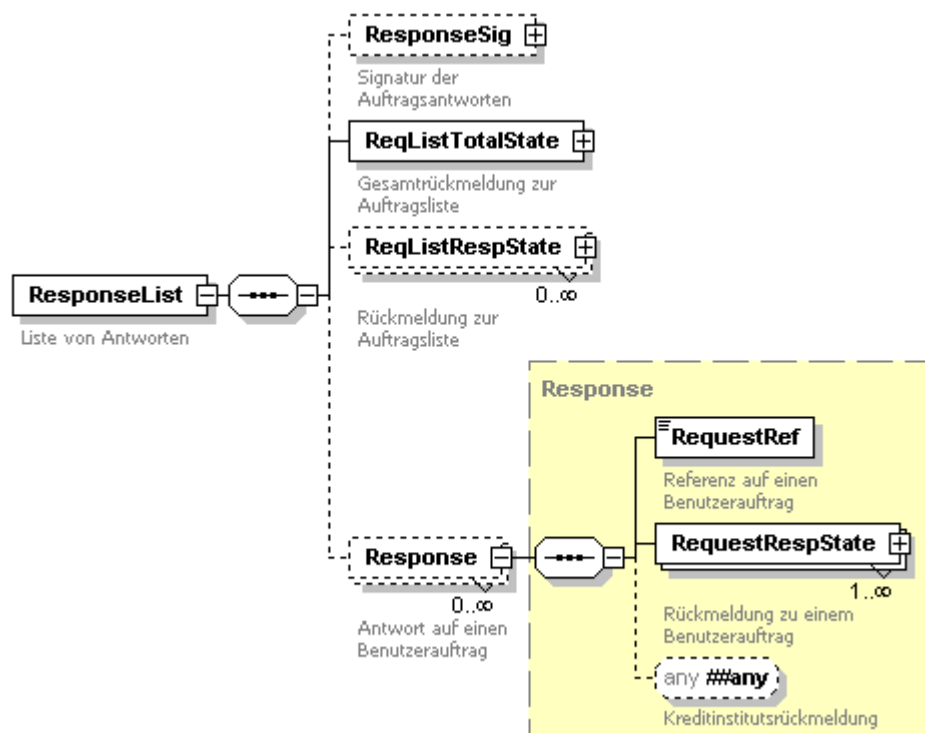


Abbildung 14: Auftragsantwort

Für die administrativen Nachrichtentypen ist das Format der Antwort fest vorgegeben.

| | | |
|-----------------|----------------------|---|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 48 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Allgemeiner Aufbau von Benutzernachricht und |

Das Element *RequestRef* ist eine Referenz auf den Benutzerauftrag. Hier ist ein XPath-Ausdruck angegeben, der die Position des zugehörigen Auftrags im Auftragsdokument relativ zu seiner *RequestList* angibt. Es gelten die folgenden Regelungen:

| | |
|---------------------|---|
| Referenz-Ziel | Wurzelement des Benutzerauftrags, auf den sich die <i>Response</i> bezieht. |
| Gültigkeitsbereich | Wurzelement der Liste von Aufträgen (<i>RequestList</i>), auf die sich die Liste der Antworten (<i>ResponseList</i>) bezieht. |
| Kontext | Wurzelement der Liste von Aufträgen (<i>RequestList</i>), auf die sich die Liste der Antworten (<i>ResponseList</i>) bezieht. |
| Zulässiger Ausdruck | Der Ausdruck in <i>XPath</i> muss der Bildungsregel für <i>RelativeLocationPath</i> genügen. |

Die Antwort enthält außerdem eine Rückmeldung *RequestRespState*, die nach dem in *III.2.2.5 Rückmeldungen zur Nachricht* beschriebenen Inhaltsmodell *ResponseState* aufgebaut ist. Belegungsrichtlinien hierfür finden sich in [Formals], Abschnitt *II.10.3 Rückmeldungen zu Aufträgen*.

Für die Belegung von *ElementRef* in *RequestRespState* gelten folgende Festlegungen:

| | |
|---------------------|--|
| Referenz-Ziel | Ein Element des Benutzerauftrags, auf den sich die Auftragsantwort bezieht. |
| Gültigkeitsbereich | Wurzelement des Benutzerauftrags, auf den sich die Auftragsantwort bezieht. |
| Kontext | Wurzelement des Benutzerauftrags, auf den sich die Auftragsantwort bezieht. |
| Zulässiger Ausdruck | Der Ausdruck in <i>XPath</i> muss der Bildungsregel für <i>RelativeLocationPath</i> genügen. |

Beispiel:

```
<ResponseList
  xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions">
  <Response>
    <RequestRef>fintstype:Orders[1]/fintstrans:SingRemitt 1 Req[1]</RequestRef>
    <RequestRespState>
      <RespCode>9110</RespCode>
      <ElementRef>fintstrans:OrderingCustAccount[1]/fintstype:BankID[1]</ElementRef>
      <RespText>Unbekannter Aufbau</RespText>
    </RequestRespState>
  </Response>
</ResponseList>
```

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten | Stand: 09.07.2004 | Seite: 49 |

III.3 Verschiedene Benutzer- und Antwortnachrichten

Dieser Abschnitt beschreibt vier der acht unterschiedlichen Nachrichtentypen: die Standard-Nachricht, die Anonyme Nachricht, die Lebendmeldung und die Synchronisierung. Die restlichen vier Nachrichtentypen sind in *III.4 Keymanagement-Nachrichten* zusammengefasst.

III.3.1 Standard-Nachricht

Die Standard-Nachricht ist derjenige Nachrichtentyp, der für den überwiegenden Teil der Kommunikation zwischen Benutzer und Kreditinstitut eingesetzt wird. In ihr können alle operativen Transaktions- und Abholaufträge aus [Messages] sowie alle administrativen Aufträge aus *III.7 Administrative Aufträge* transportiert werden. Die Verwendung der Auftrags- und Antwortteile, Verschlüsselung, Signatur und Initialisierung ist unter [Formals], Abschnitt *II.9 Benutzernachrichten allgemein* beschrieben.

Eine Standard-Kreditinstitutsnachricht kann auch als Antwort auf andere Nachrichtentypen verwendet werden, wenn in einem Fehlerfall die Benutzernachricht nicht interpretierbar ist. In solchen Fällen darf die Kreditinstitutsnachricht keine Auftragsantworten, sondern nur eine Fehlerrückmeldung zur Gesamtnachricht enthalten.

a) Benutzernachricht

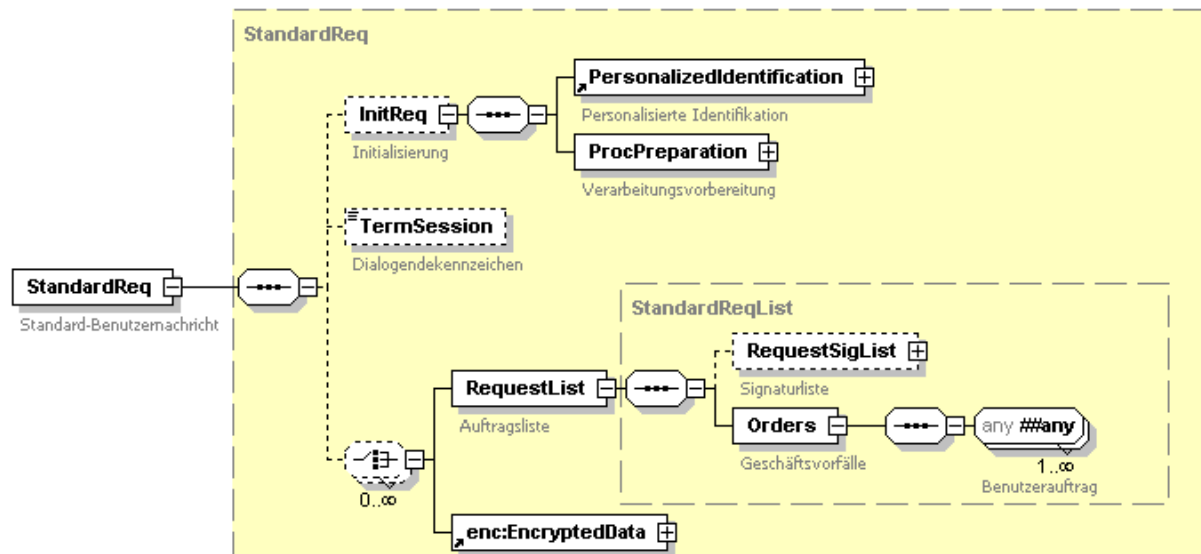


Abbildung 15: Standard-Benutzernachricht

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 50 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten |

b) Kreditinstitutsnachricht

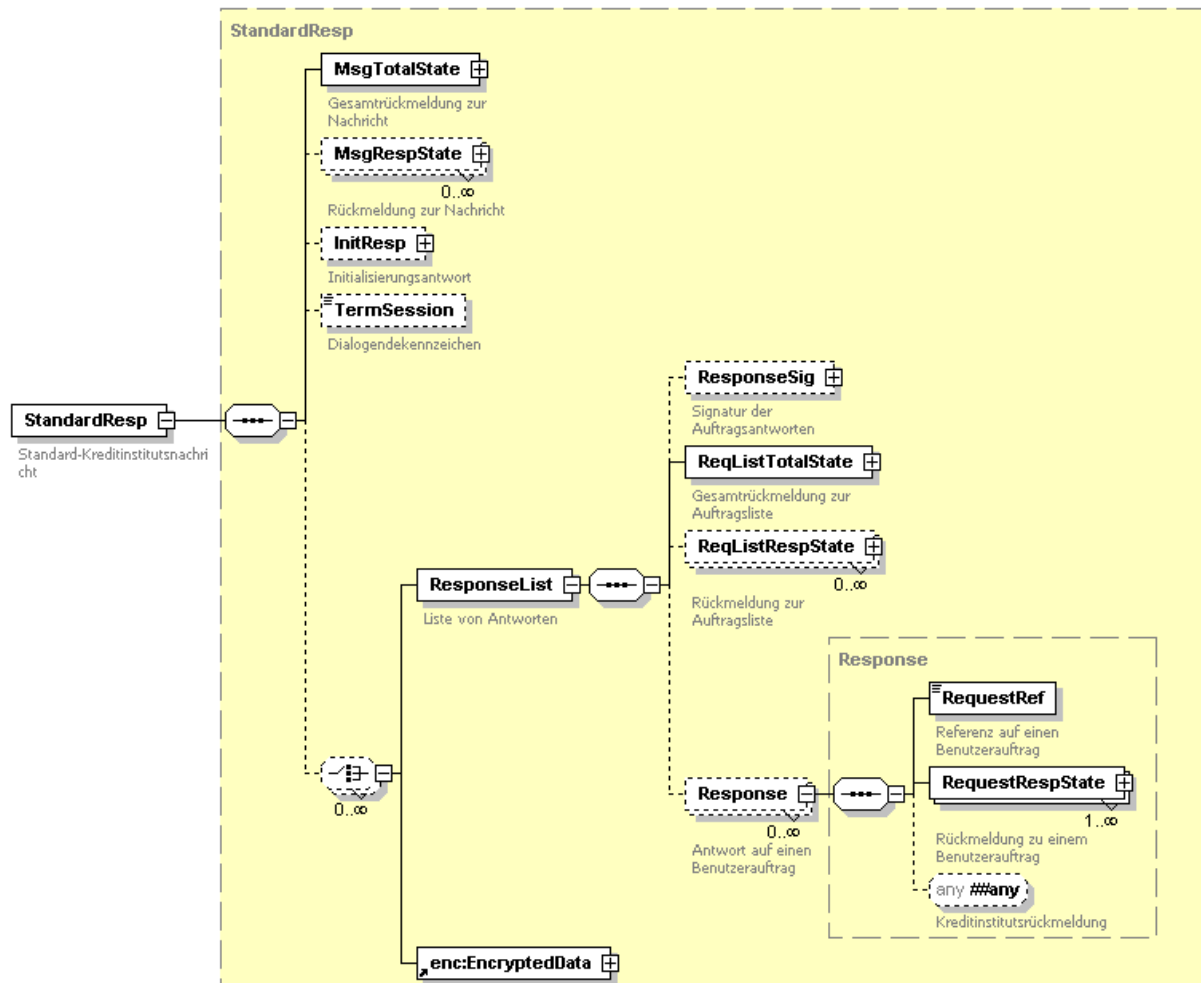


Abbildung 16: Standard-Kreditinstitutsnachricht

III.3.2 Anonyme Nachricht

Bei anonymer Kommunikation nach [Formals], Abschnitt II.17 *Anonymer Zugang* werden Nachrichten nicht verschlüsselt und nicht signiert, Komprimierung ist allerdings möglich. Der sonstige Aufbau entspricht der Standard-Nachricht.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten | Stand: 09.07.2004 | Seite: 51 |

a) Benutzernachricht

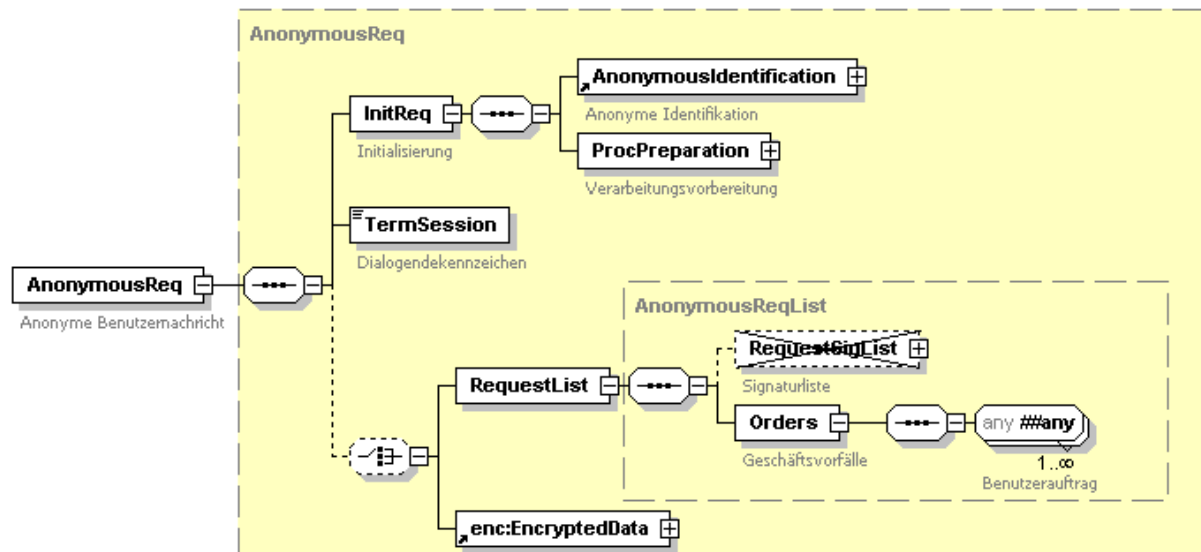


Abbildung 17: Anonyme Benutzernachricht

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 52 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten |

b) Kreditinstitutsnachricht

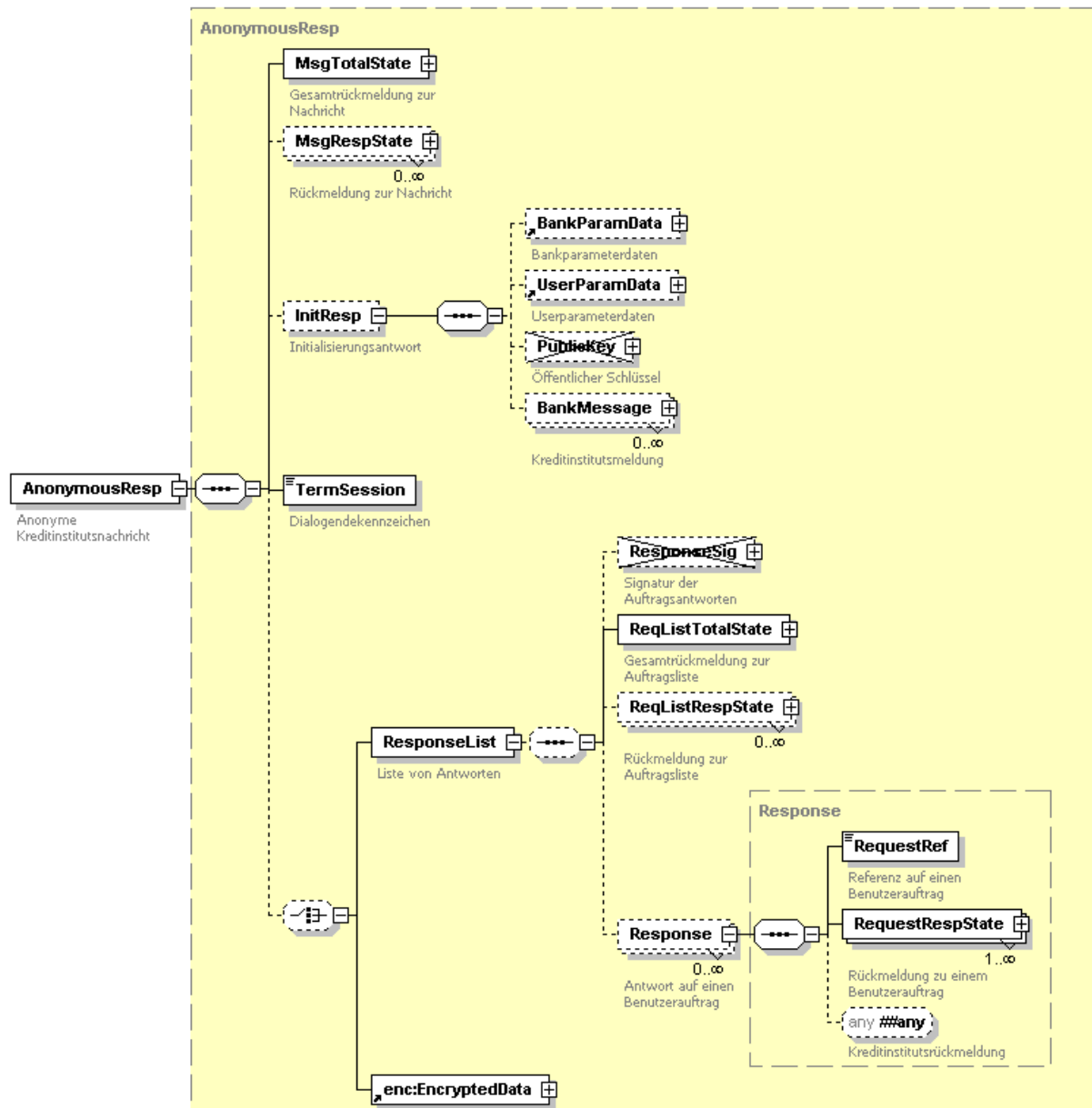


Abbildung 18: Anonyme Kreditinstitutsnachricht

Die Initialisierungsantwort der anonymen Kreditinstitutsnachricht enthält keine öffentlichen Kreditinstitutsschlüssel.

III.3.3 Lebendmeldung

Die Lebendmeldungs-nachricht dient zur Vermeidung eines kreditinstitutsseitigen Verbindungsabbruchs bei Zeitüberschreitung in einem synchronen Dialog (siehe [Formals], Abschnitt III.6 Lebendmeldung in Dialogen). Der Nachrichtenkörper ist sowohl in der Benutzernachricht als auch in der Kreditinstitutsnachricht leer, sowohl Nachricht als auch Antwort sind anonym.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten | Stand: 09.07.2004 | Seite: 53 |

a) Benutzernachricht

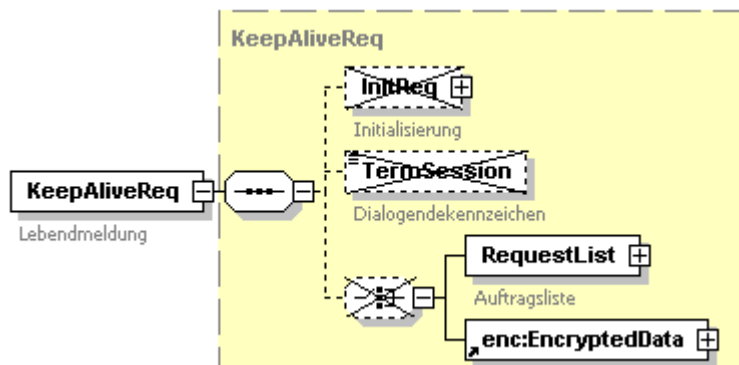


Abbildung 19: Benutzernachricht Lebendmeldung

Es gelten besondere Belegungsrichtlinie für den Nachrichtenkopf einer Lebendmeldung (nicht in der Abbildung gezeigt):

Nachrichtennummer

Ist mit der Nummer 0 zu belegen.

Textuelle Referenz des Benutzers

Bei dieser Nachricht muss die textuelle Referenz nicht eindeutig sein, da die Nachricht nicht im Statusprotokoll vermerkt wird.

b) Kreditinstitutsnachricht

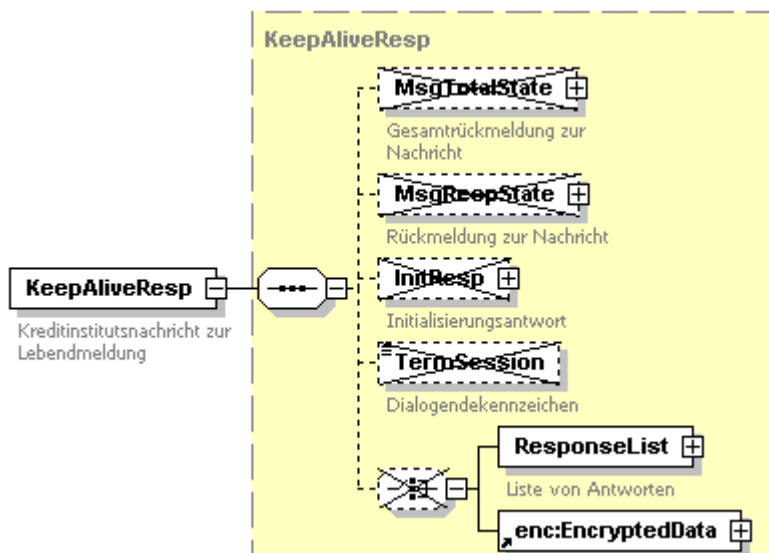


Abbildung 20: Kreditinstitutsnachricht zur Lebendmeldung

Diese Nachricht kann keine Rückmeldungen transportieren. Falls der Dialog bei Eintreffen der Lebendmeldung bereits geschlossen ist, antwortet das Institut mit einer Standard-Kreditinstitutsnachricht mit entsprechender Fehlermeldung.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 54 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten |

III.3.4 Synchronisierung

Die Synchronisierung ([Formals], Abschnitt *III.3 Synchronisierung*) dient zum Abgleich verschiedener beim Benutzer und/oder beim Institut geführter Informationen und Zählerwerte.

a) Benutzernachricht

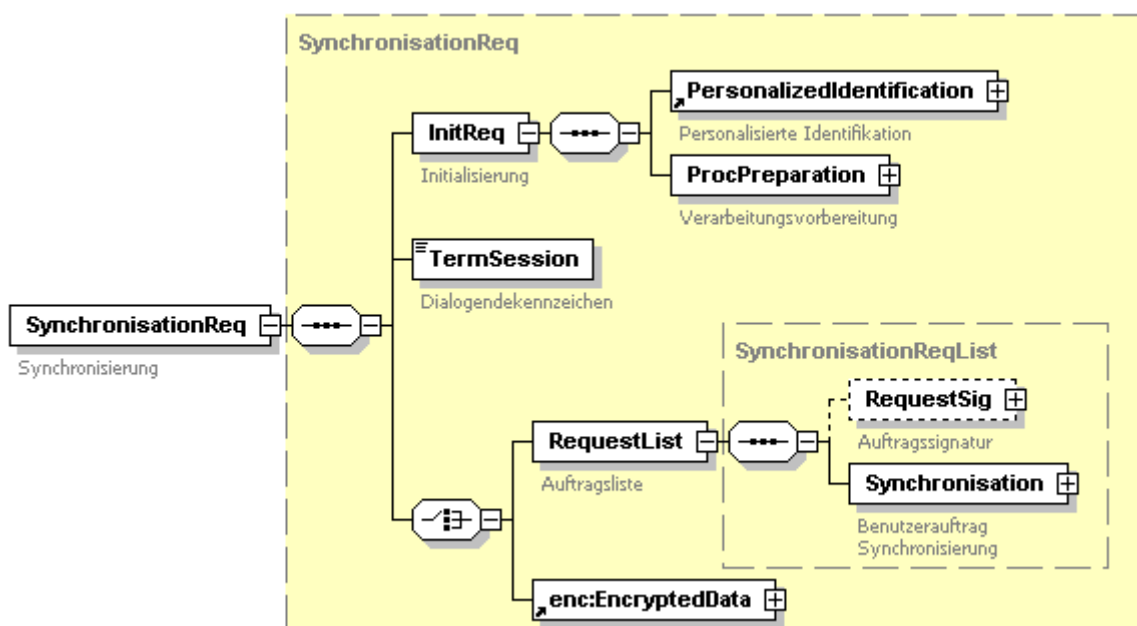


Abbildung 21: Benutzernachricht Synchronisierung

In die Auftragsliste kann ausschließlich der Auftragstyp „Benutzerauftrag Synchronisierung“ eingestellt werden:

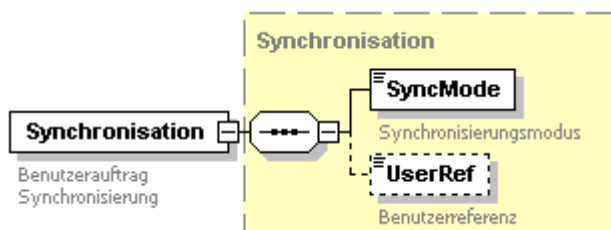


Abbildung 22: Benutzerauftrag Synchronisierung

Zu diesem Auftrag gibt es keine geschäftsvorfallspezifischen Parameter. Der Auftrag kann durch das Kreditinstitut im Rahmen der BPD nicht ausgeschlossen werden, in den UPD wird er nicht aufgeführt.

Benutzerreferenz

Das Element *UserRef* darf nur im Synchronisierungsmodus *SyncMode* = 3 eingestellt werden.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Verschiedene Benutzer- und Antwortnachrichten | Stand: 09.07.2004 | Seite: 55 |

b) Kreditinstitutsnachricht

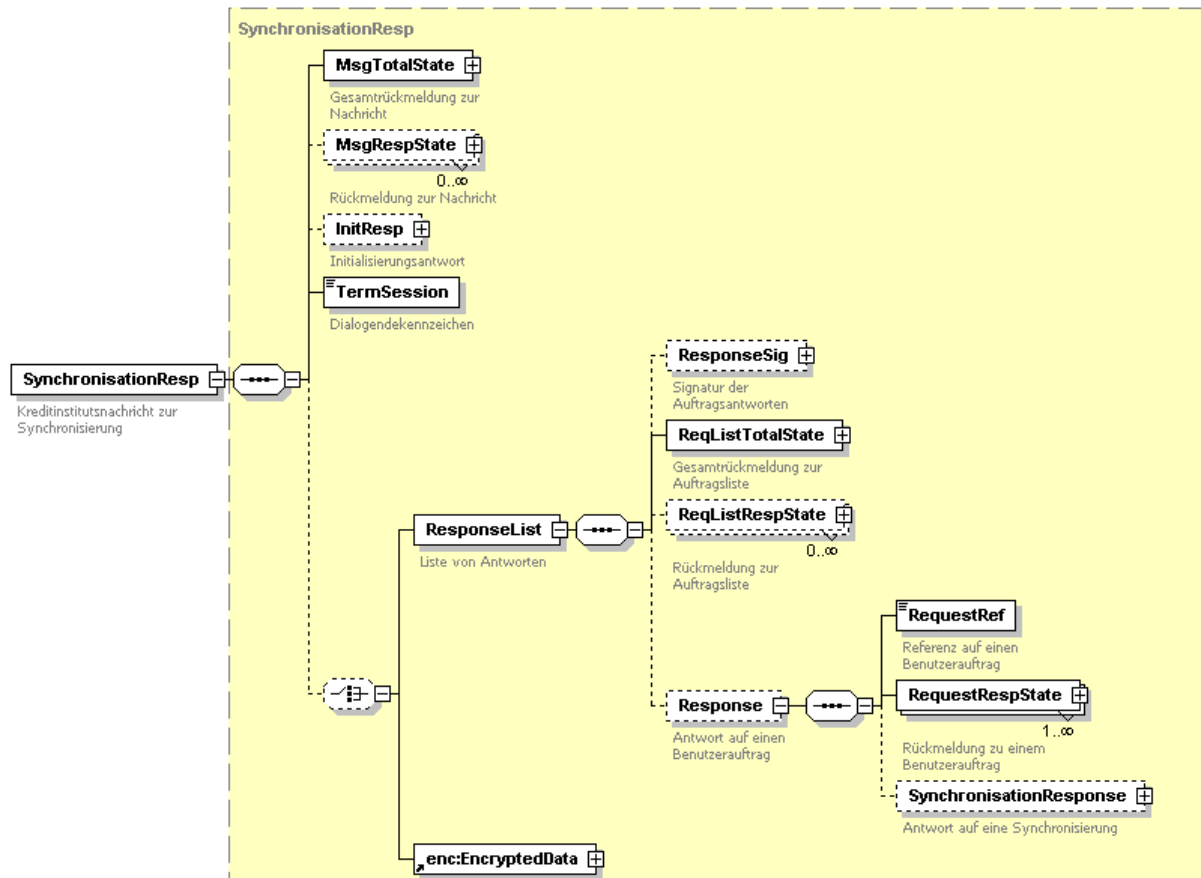


Abbildung 23: Kreditinstitutsnachricht zur Synchronisierung

In die Liste von Antworten kann ausschließlich der Auftragstyp „Antwort auf eine Synchronisierung“ eingestellt werden:

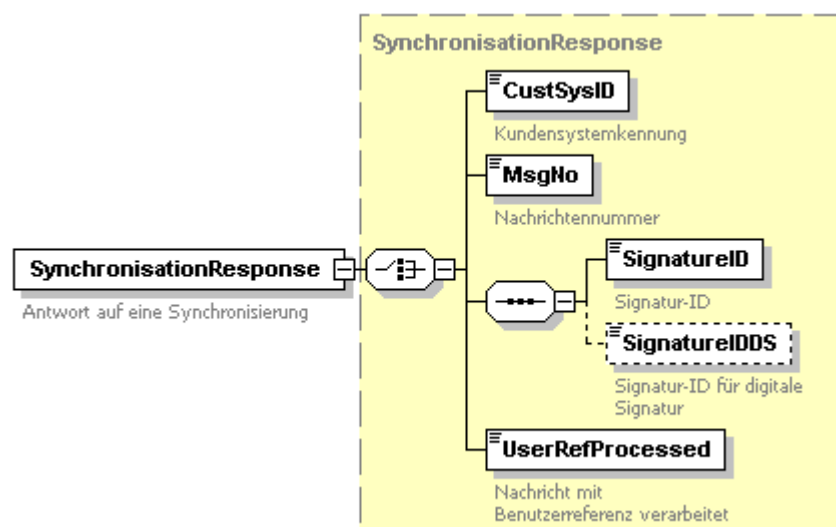


Abbildung 24: Antwort auf eine Synchronisierung

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 56 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

III.4 Keymanagement-Nachrichten

Das Sicherheitsverfahren [HBCI] kennt vier administrative Geschäftsvorfälle zur Schlüsselverwaltung. Da diese nicht mit anderen Geschäftsvorfällen in einem Dialog gemischt werden dürfen und da sie teilweise besondere Anforderungen an Signatur und Verschlüsselung stellen, sind in der FinTS-Syntax dafür vier spezielle Nachrichtentypen definiert. Jeder Auftrag des Keymanagements darf nur in seinem zugehörigen Nachrichtentyp transportiert werden, umgekehrt können diese Nachrichtentypen keine anderen Geschäftsvorfälle aufnehmen. Zu diesen administrativen Aufträgen gibt es keine geschäftsvorfallspezifischen Parameter. Sie können durch das Kreditinstitut im Rahmen der BPD nicht ausgeschlossen werden, in den UPD werden sie nicht aufgeführt.

III.4.1 Anforderung der Kreditinstitutsschlüssel

Diese Nachricht dient im RDH-Verfahren dazu, die öffentlichen Schlüssel des Kreditinstituts zum Benutzer zu übertragen. Sowohl Auftrag als auch Antwort sind unverschlüsselt. Die Benutzernachricht ist unsigniert, die Kreditinstitutsnachricht ist mit dem im Auftrag übertragenen Schlüssel signiert, falls das Kreditinstitut seine Nachrichten signiert. Komprimierung ist in beiden Richtungen möglich. Siehe [HBCI], Abschnitt II.6.1.2 *Erstmalige Anforderung der Schlüssel des Kreditinstituts*.

a) Auftrag

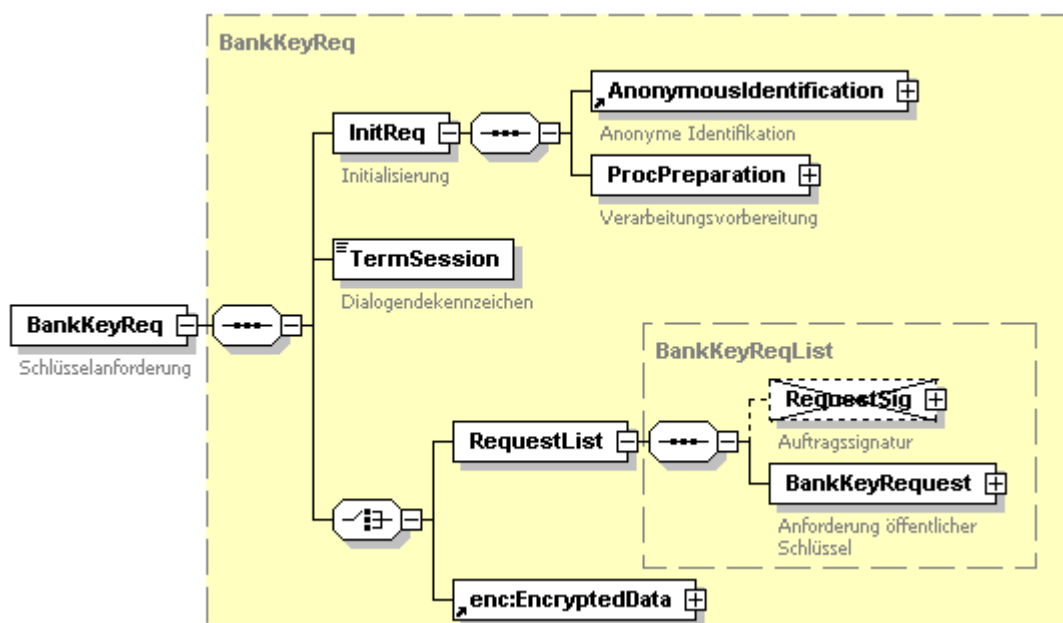


Abbildung 25: Benutzernachricht Anforderung der Kreditinstitutsschlüssel

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 57 |

In die Auftragsliste kann ausschließlich der Auftragstyp „Anforderung öffentlicher Schlüssel“ eingestellt werden:

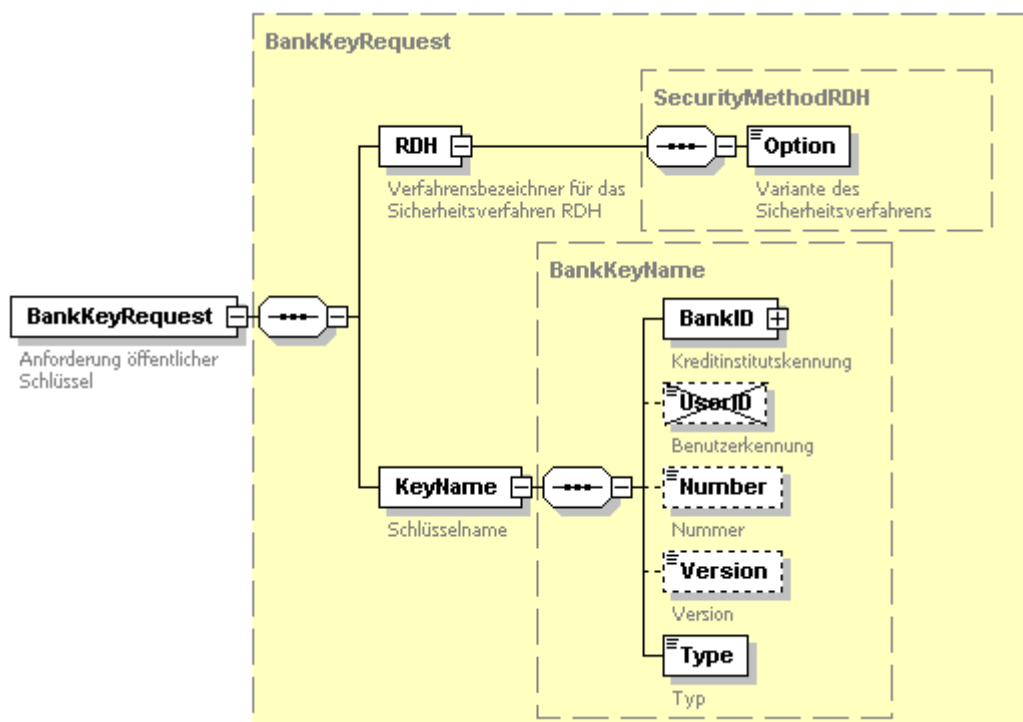


Abbildung 26: Anforderung öffentlicher Schlüssel

Schlüsselname

Wenn bekannt, werden hier Nummer und Version der aktuellen Kreditinstitutsschlüssel eingestellt. Werden mit Nummer und Version bereits abgelaufene Schlüssel bezeichnet, obliegt es dem Kreditinstitut, ob es diese oder die aktuellen Schlüssel sendet, siehe [HBCI], Abschnitt II.6.1.2 *Erstmalige Anforderung der Schlüssel des Kreditinstituts*.

Typ

Es wird immer „S“ für den Signierschlüssel angegeben. Das Kreditinstitut sendet in der Antwort einen oder beide Schlüssel, siehe auch [HBCI], Abschnitt II.6.1.2 *Erstmalige Anforderung der Schlüssel des Kreditinstituts*. Über den bei RDH-3 und RDH-4 vorhandenen dritten Schlüssel für die digitale Signatur verfügt das Kreditinstitut nicht.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 58 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

b) Antwort

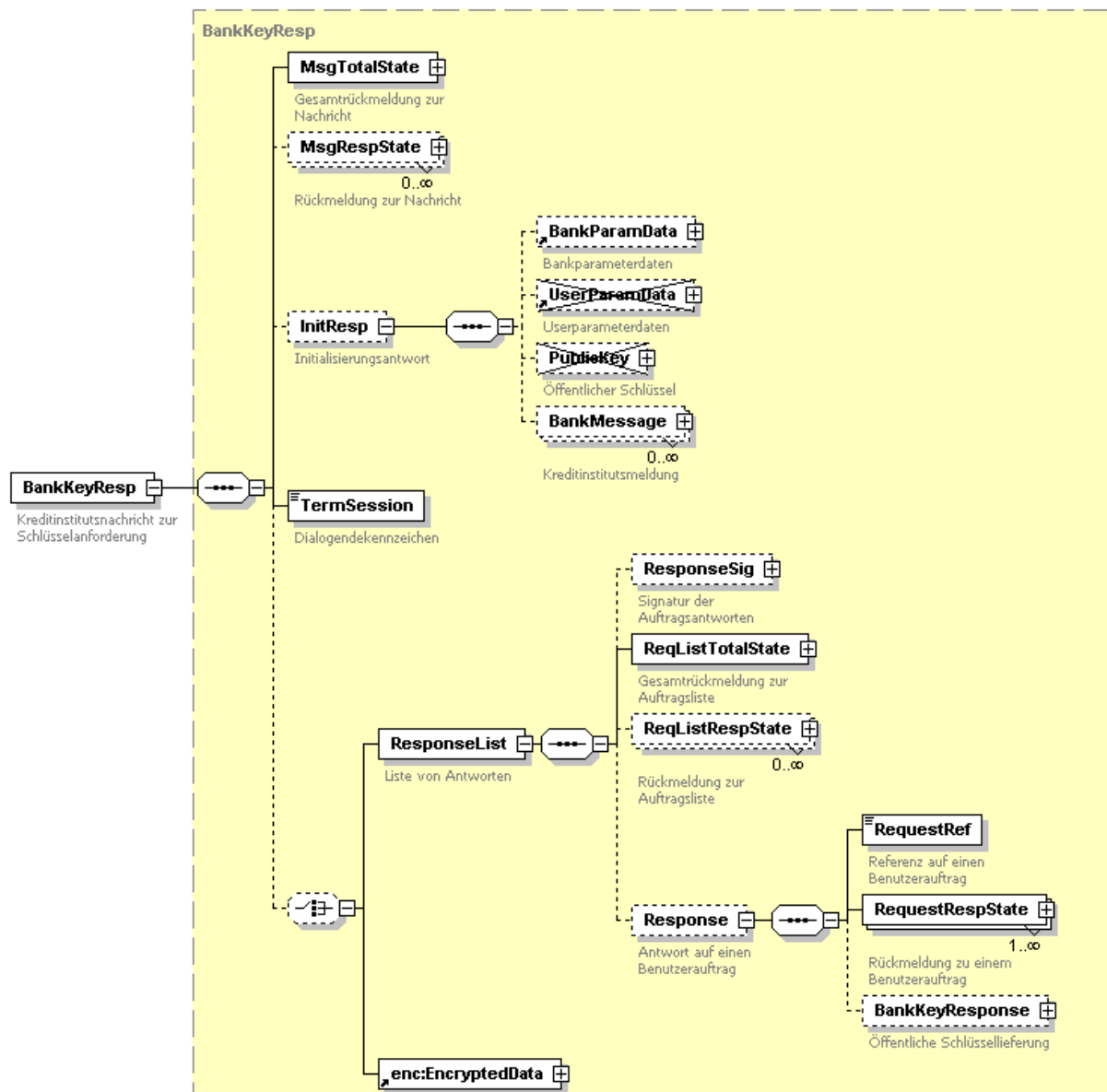


Abbildung 27: Kreditinstitutsnachricht Anforderung der Kreditinstitutsschlüssel

Die Initialisierungsantwort der Kreditinstitutsnachricht enthält keine User-Parameterdaten und keine öffentlichen Kreditinstitutsschlüssel.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 59 |

In die Liste von Antworten kann ausschließlich der Auftragsstyp „Öffentliche Schlüssellieferung“ eingestellt werden:

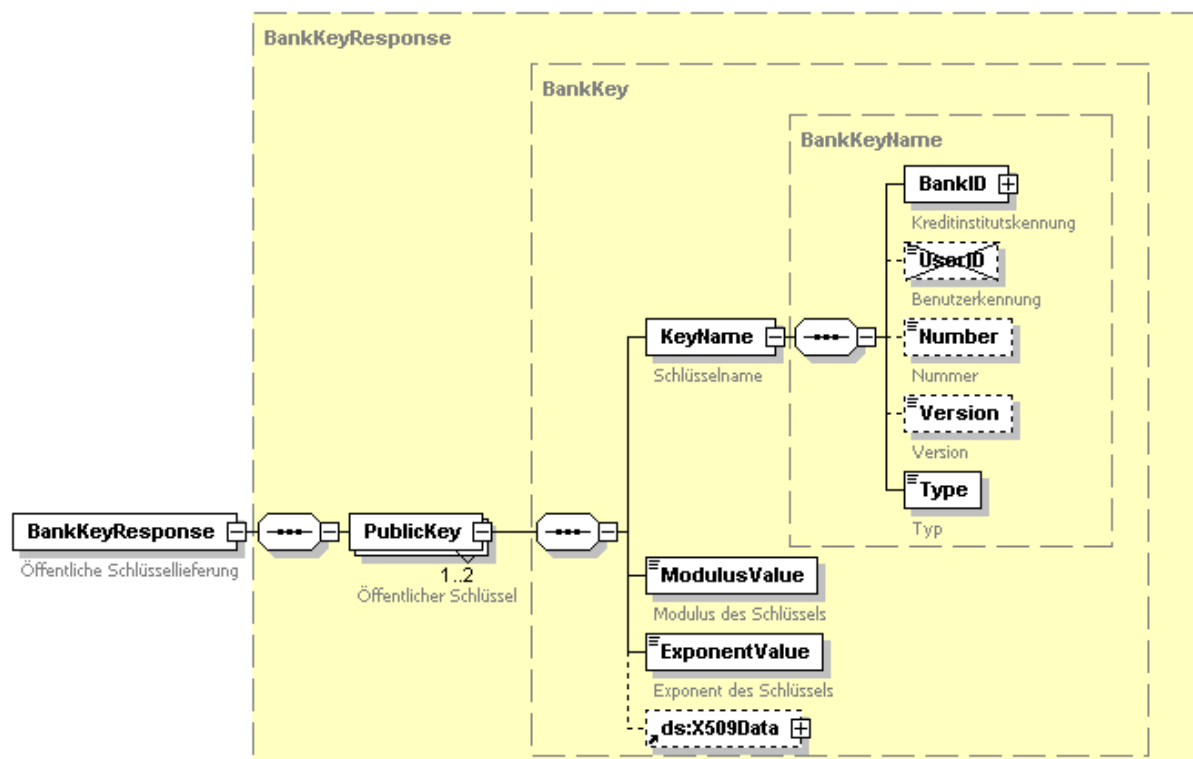


Abbildung 28: Öffentliche Schlüssellieferung

III.4.2 Erstmalige Übermittlung eines Kundenschlüssels

Mit einer Nachricht dieses Typs übermittelt der Benutzer im Rahmen der RDH-Erstinitialisierung seine öffentlichen Schlüssel an das Kreditinstitut. Die Benutzernachricht ist verschlüsselt und bereits mit dem übertragenen Signierschlüssel signiert, die Kreditinstitutsantwort ist im Erfolgsfall signiert, aber nicht verschlüsselt. Komprimierung ist in beiden Richtungen möglich. Siehe [HBCI], Abschnitt II.6.1.3 *Erstmalige Übermittlung der Schlüssel des Benutzers*.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 60 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

a) Auftrag

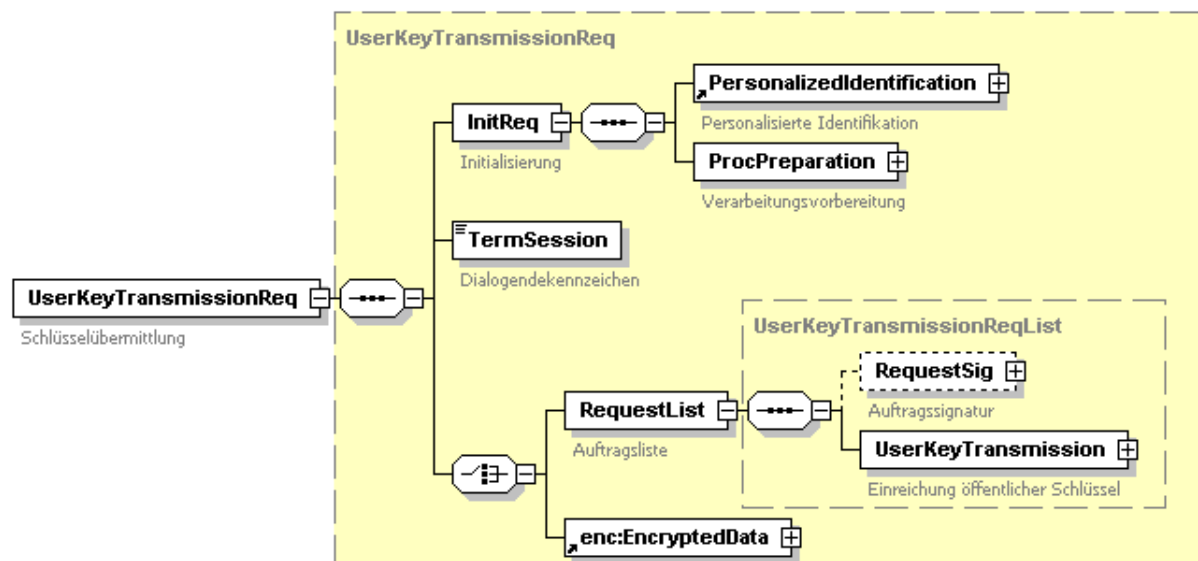


Abbildung 29: Benutzernachricht Übermittlung eines Kundenschlüssels

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 61 |

In die Auftragsliste kann ausschließlich der Auftragstyp „Einreichung öffentlicher Schlüssel“ eingestellt werden:

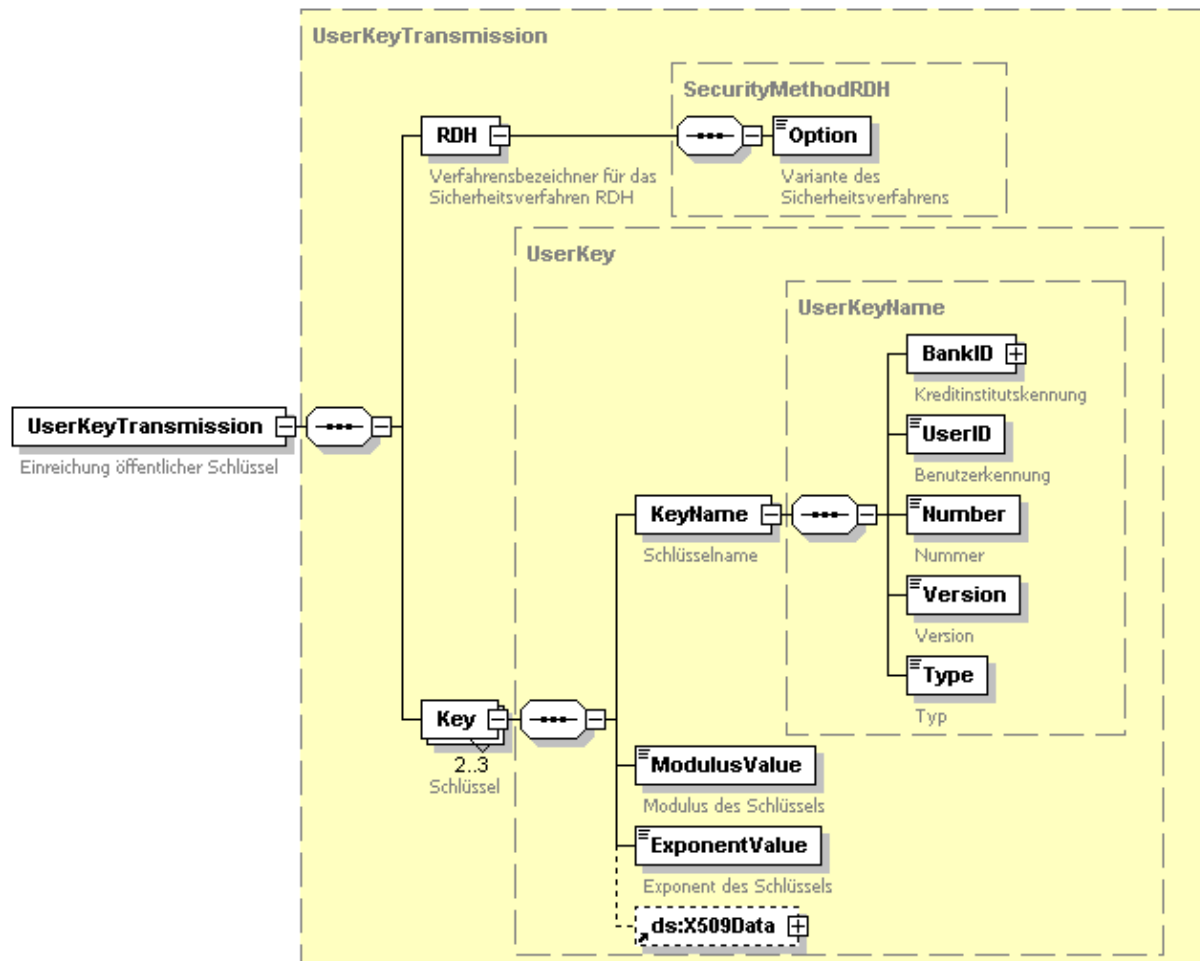


Abbildung 30: Einreichung öffentlicher Schlüssel

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 62 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

b) Antwort

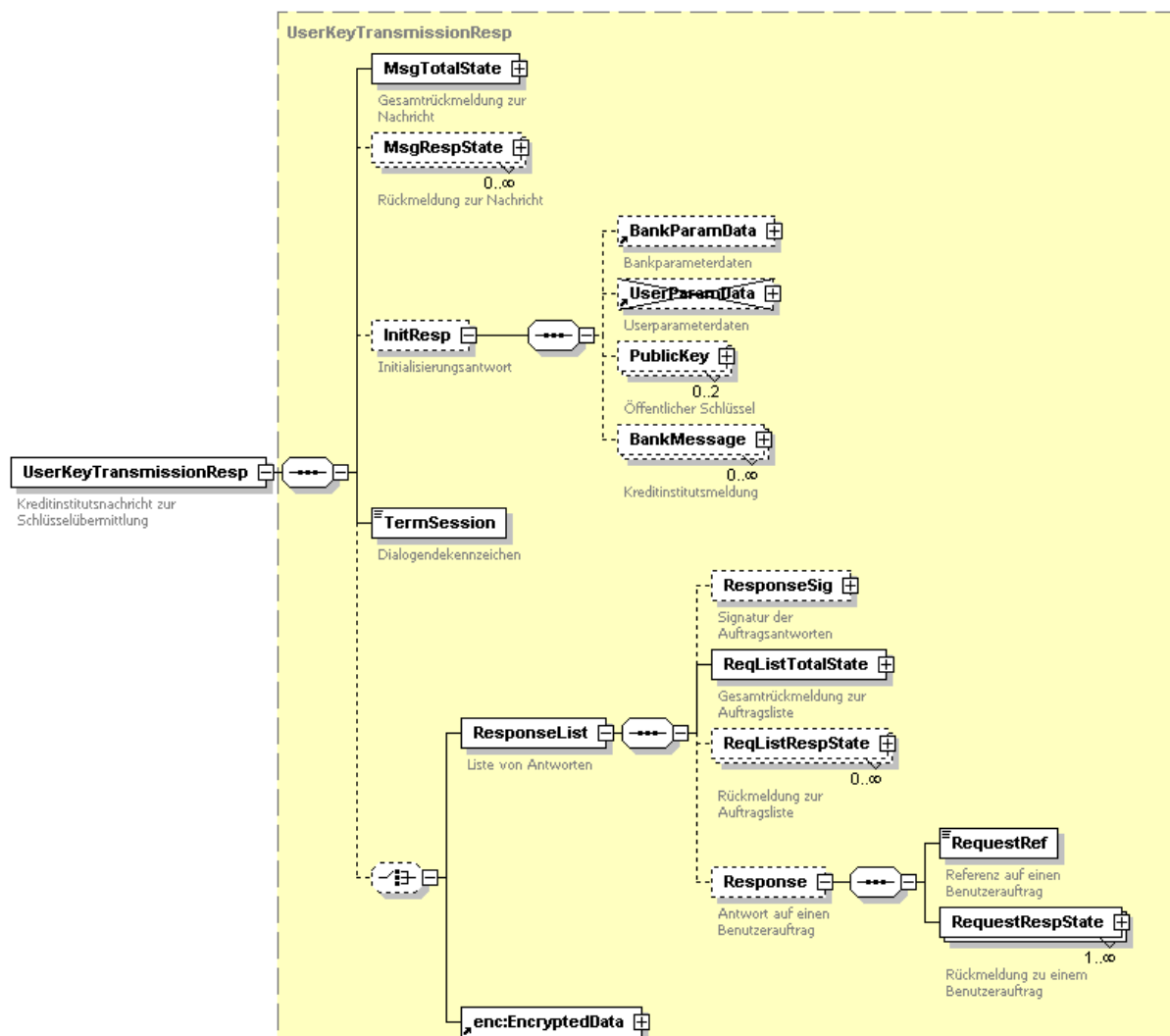


Abbildung 31: Kreditinstitutsnachricht zur Übermittlung eines Kundenschlüssels

Die Initialisierungsantwort der Kreditinstitutsnachricht enthält keine User-Parameterdaten.

Die Antwortnachricht meldet außer dem *RequestRespState* keine weiteren Daten zurück.

III.4.3 Schlüsseländerung

Im RDH-Verfahren kann der Benutzer mit diesem Nachrichtentyp seine Schlüssel wechseln. Beide Nachrichten sind personalisiert, insbesondere ist die Antwort im Erfolgsfall bereits mit dem neuen Benutzerschlüssel verschlüsselt. Komprimierung ist in beiden Richtungen möglich. Siehe [HBCI], Abschnitt 11.6.1.1 *Änderung eines öffentlichen Schlüssels des Benutzers*.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 63 |

a) Auftrag

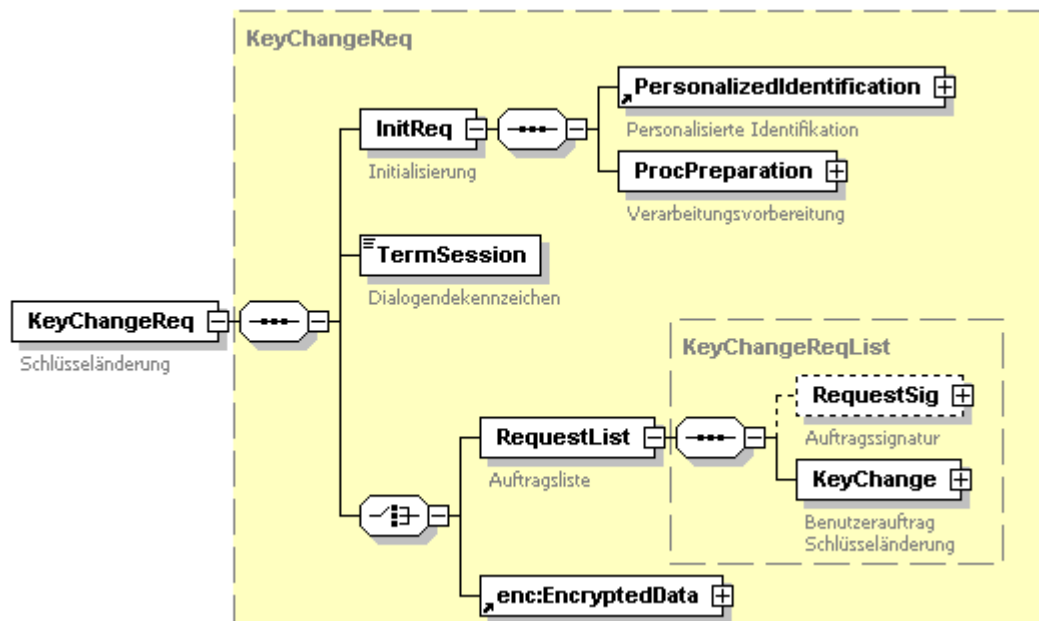


Abbildung 32: Benutzernachricht Schlüsseländerung

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 64 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

In die Auftragsliste kann ausschließlich der Auftragstyp „Benutzerauftrag Schlüsseländerung“ eingestellt werden:

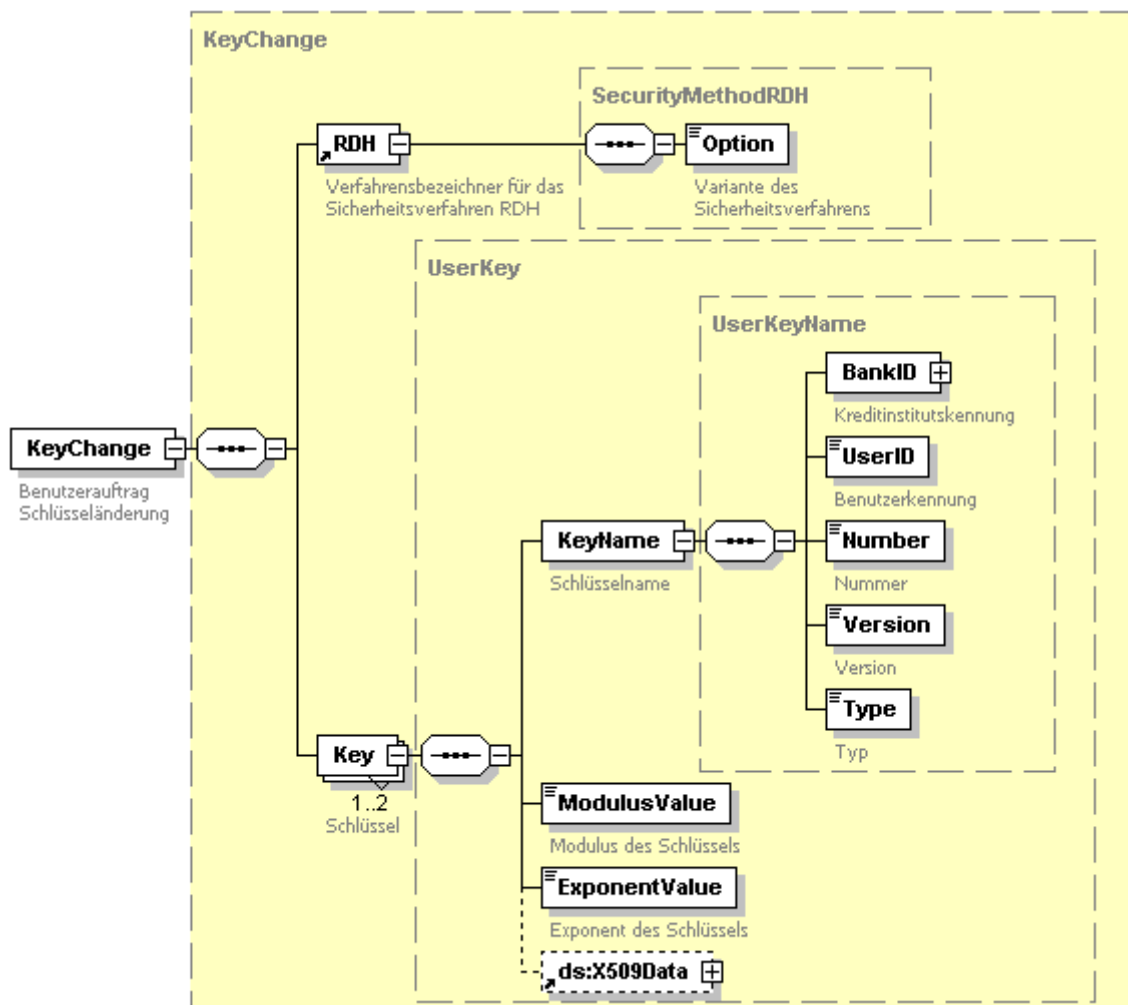


Abbildung 33: Benutzerauftrag Schlüsseländerung

RDH

Verfahren, für das der neue Schlüssel (die neuen Schlüssel) gilt (gelten).

Schlüssel

Es können bis zu zwei zu ändernde Schlüssel gleichzeitig angegeben werden. Der im Verfahren RDH-3 und RDH-4 definierte zusätzliche Schlüssel für digitale Signatur kann nicht geändert werden.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 65 |

b) Antwort

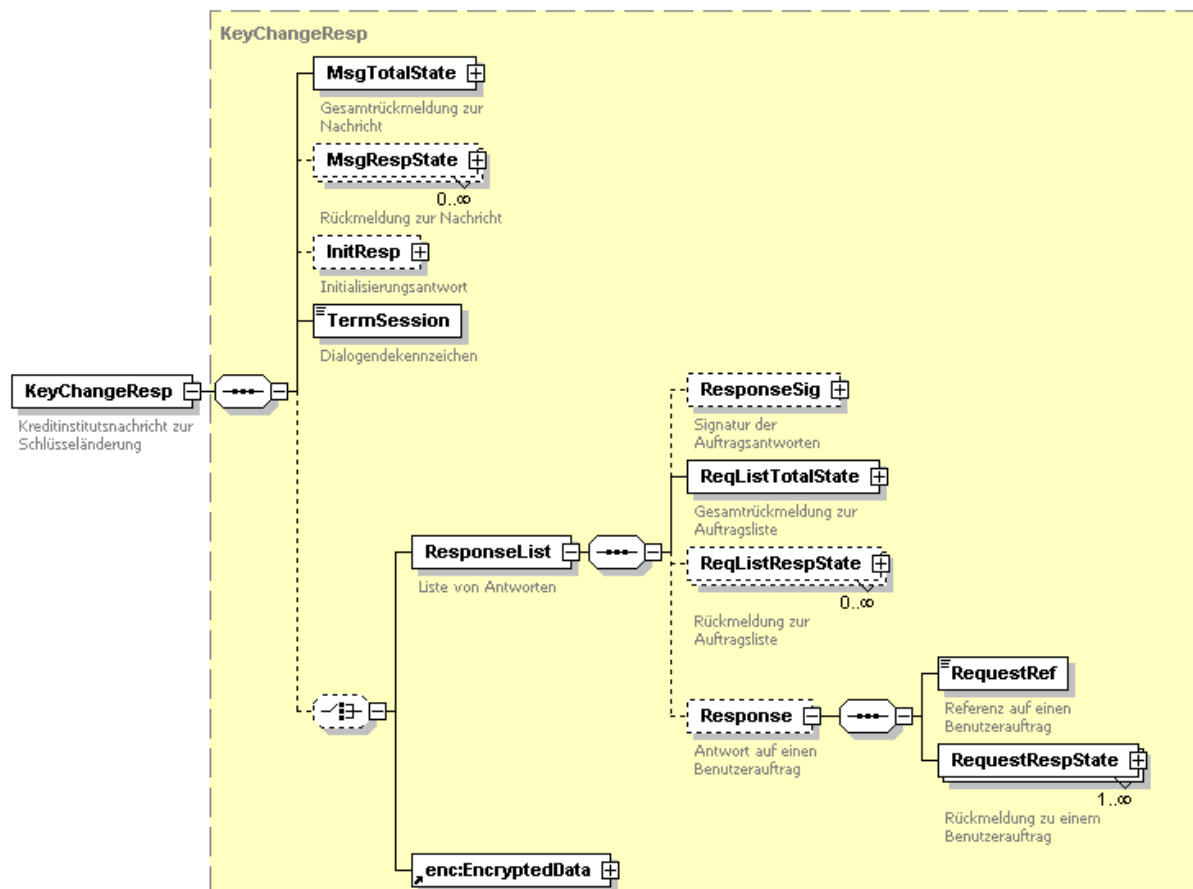


Abbildung 34: Kreditinstitutsnachricht zur Schlüsseländerung

Die Antwortnachricht meldet außer dem *RequestRespState* keine weiteren Daten zurück.

III.4.4 Schlüsselsperrung

Mit dieser Nachricht kann ein Benutzer sowohl im RDH- als auch im DDV-Verfahren seine Schlüssel sperren. Die Benutzernachricht ist personalisiert, die Kreditinstitutsnachricht ist bei erfolgreicher Sperrung je nach Sicherheitsverfahren teilweise oder vollständig anonym. Komprimierung ist in beiden Richtungen möglich. Siehe [HBCI], Abschnitt II.6.1.4 *Schlüsselsperrung durch den Benutzer*.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 66 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

a) Auftrag

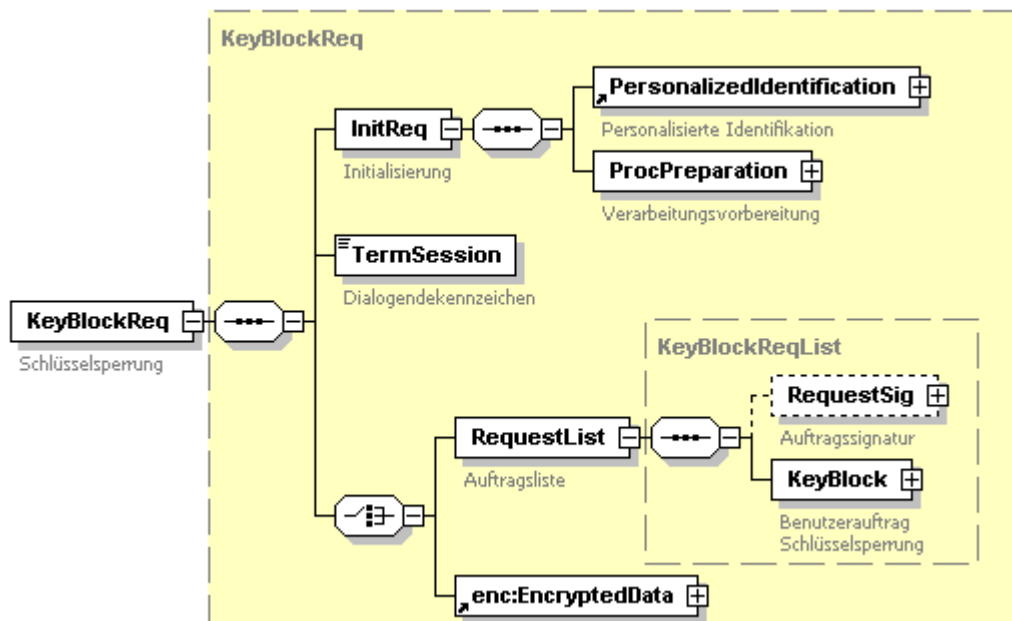


Abbildung 35: Benutzernachricht Schlüsselsperung

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten | Stand: 09.07.2004 | Seite: 67 |

In die Auftragsliste kann ausschließlich der Auftragstyp „Benutzerauftrag Schlüsselsperrung“ eingestellt werden:

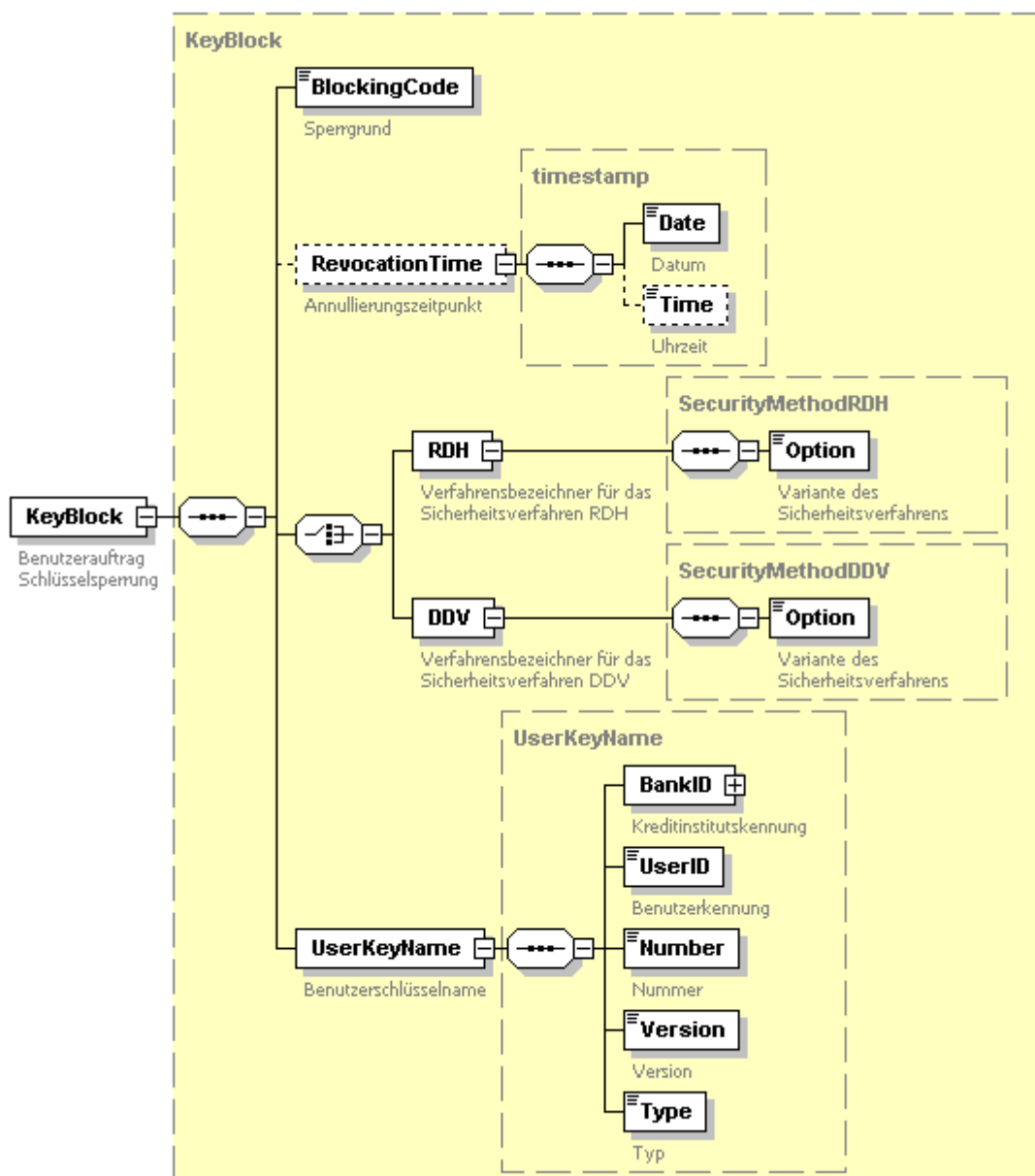


Abbildung 36: Benutzerauftrag Schlüsselsperrung

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 68 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Keymanagement-Nachrichten |

b) Antwort

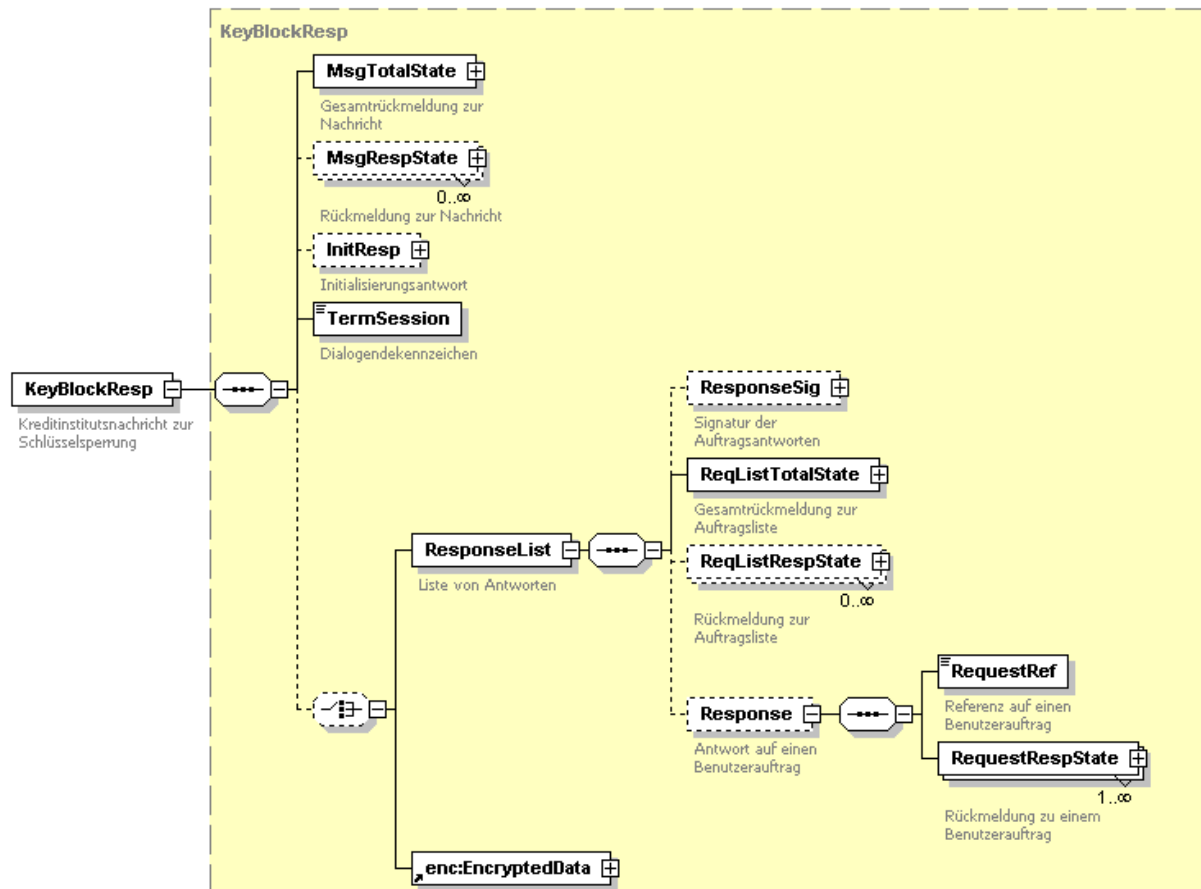


Abbildung 37: Kreditinstitutsnachricht zur Schlüsselspernung

Die Antwortnachricht meldet außer dem *RequestRespState* keine weiteren Daten zurück.

| | | |
|--|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Bankparameterdaten | Stand: 09.07.2004 | Seite: 69 |

III.5 Bankparameterdaten

In den Bankparameterdaten (BPD) legt das Kreditinstitut den unterstützten Leistungsumfang fest und beschreibt diesen durch Parameter (siehe [FORMALS], Abschnitt IV. *BANKPARAMETERDATEN (BPD)*). Die BPD werden entweder in der Initialisierungsantwort zum Benutzer übertragen oder als Antwort auf einen administrativen Abruf-Auftrag (siehe III.2.2.3 *Initialisierungsantwort*, III.7 *Administrative Aufträge*). Die Bankparameterdaten sind in mehrere Segmente unterteilt, die im Folgenden gezeigt werden.

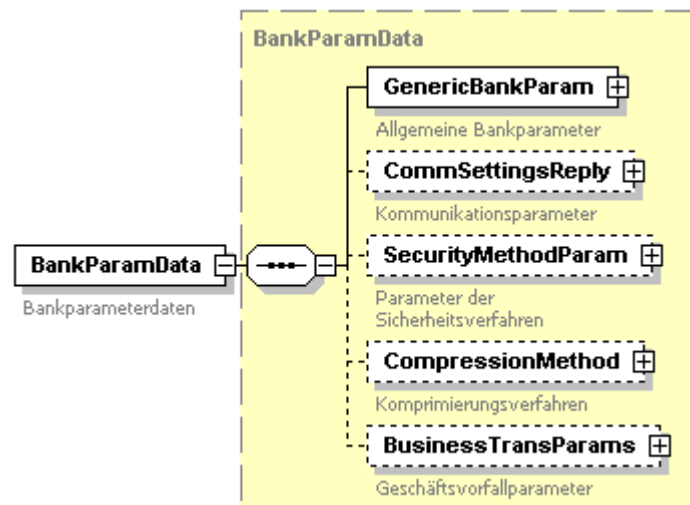


Abbildung 38: Bankparameterdaten

a) Allgemeine Bankparameter

Dieses Segment enthält allgemeine Informationen zum Kreditinstitut und zur unterstützten FinTS-Version.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 70 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Bankparameterdaten |

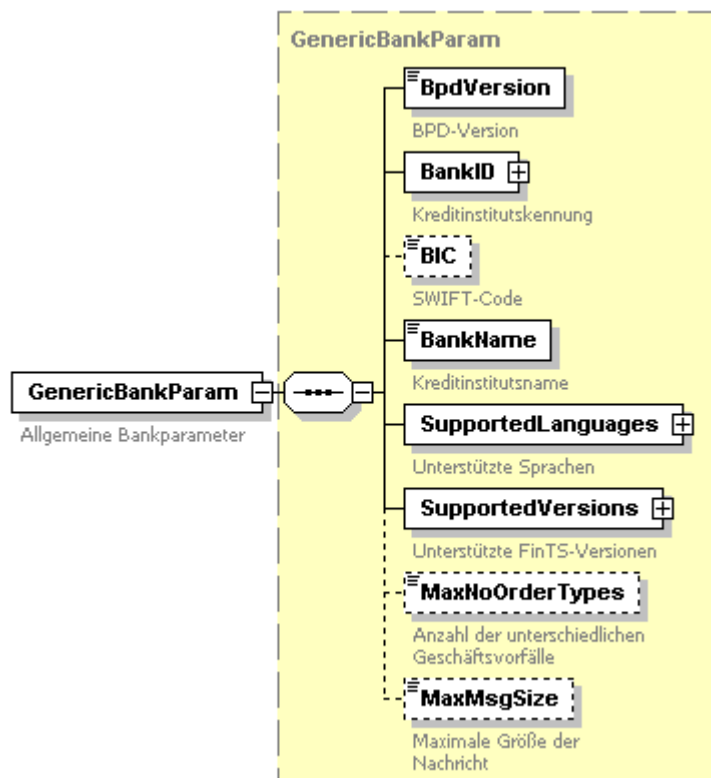


Abbildung 39: Allgemeine Bankparameterdaten

b) Kommunikationsparameter

Dieses Segment enthält Informationen zu den möglichen Kommunikationsverbindungen mit dem Kreditinstitut.

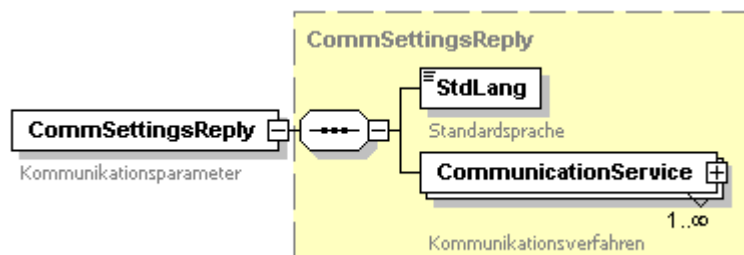


Abbildung 40: Kommunikationsparameter

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Bankparameterdaten | Stand: 09.07.2004 | Seite: 71 |

Das Kommunikationsverfahren definiert spezifische Parameter eines Transportprotokolls:

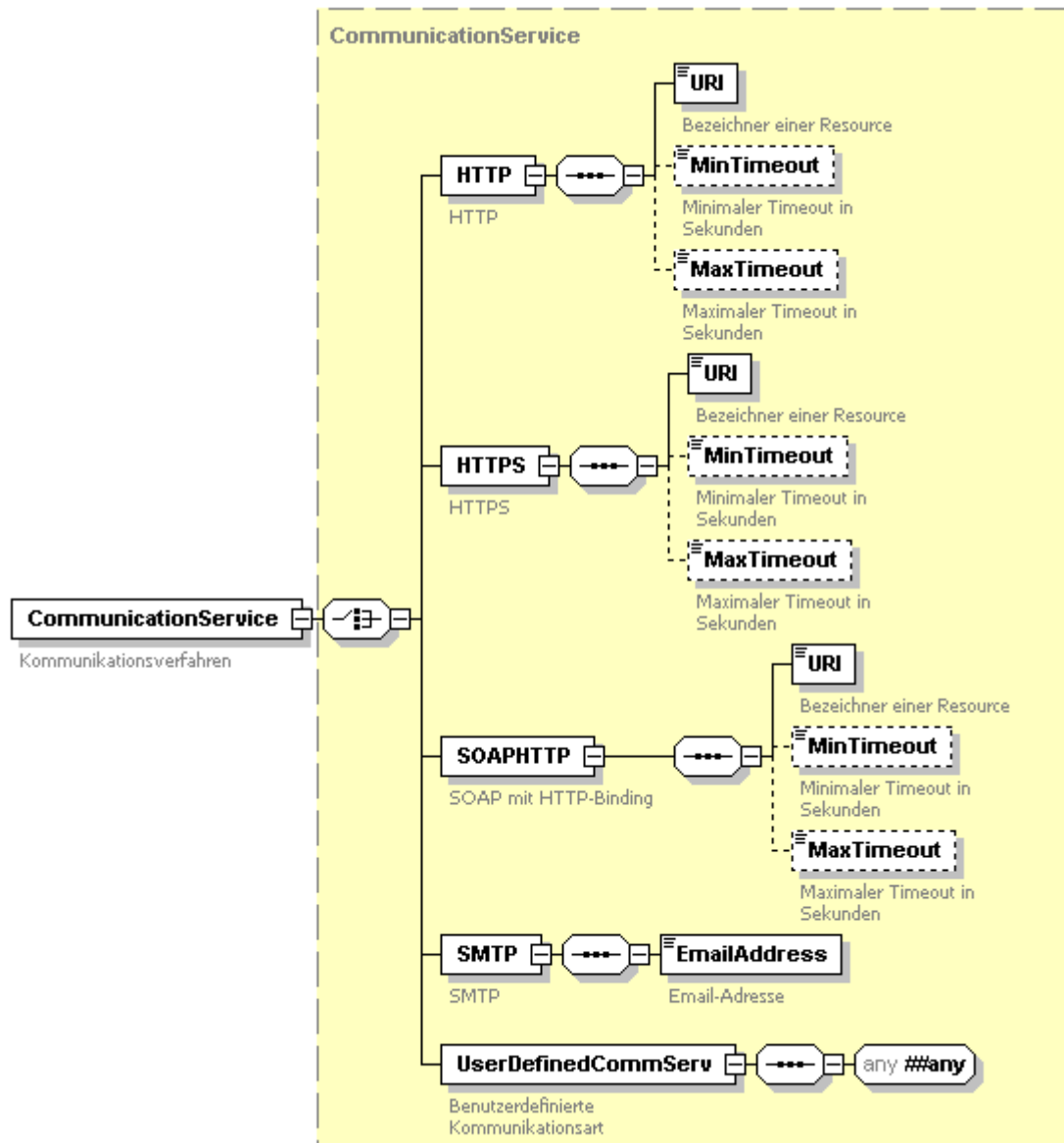


Abbildung 41: Kommunikationsverfahren

c) Parameter der Sicherheitsverfahren

In diesem Segment der BPD gibt das Kreditinstitut die unterstützten Sicherheitsverfahren und ihre Parameter an. Wenn ein Verfahren nicht unterstützt wird, ist es in der Aufzählung nicht vorhanden, ansonsten zählt zu seinen Parametern auch die Festlegung der mit diesem Verfahren signierbaren Geschäftsvorfälle. Die Geschäftsvorfälle können dabei entweder in Listen nach Namensraum sortiert aufgezählt oder aber generell zugelassen werden.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 72 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Bankparameterdaten |

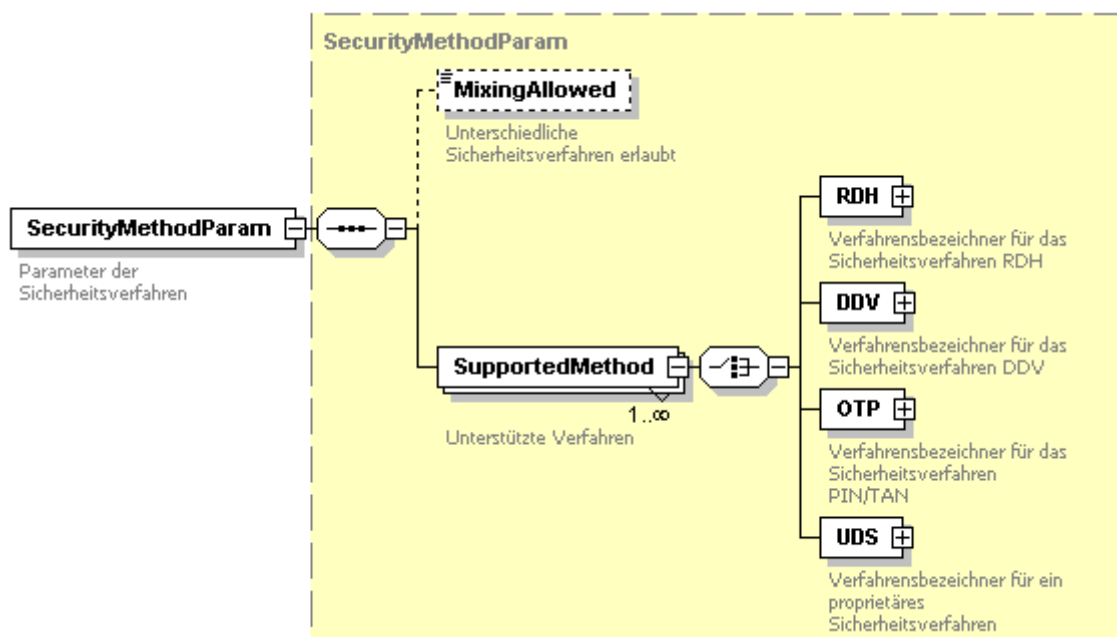


Abbildung 42: Parameter der Sicherheitsverfahren

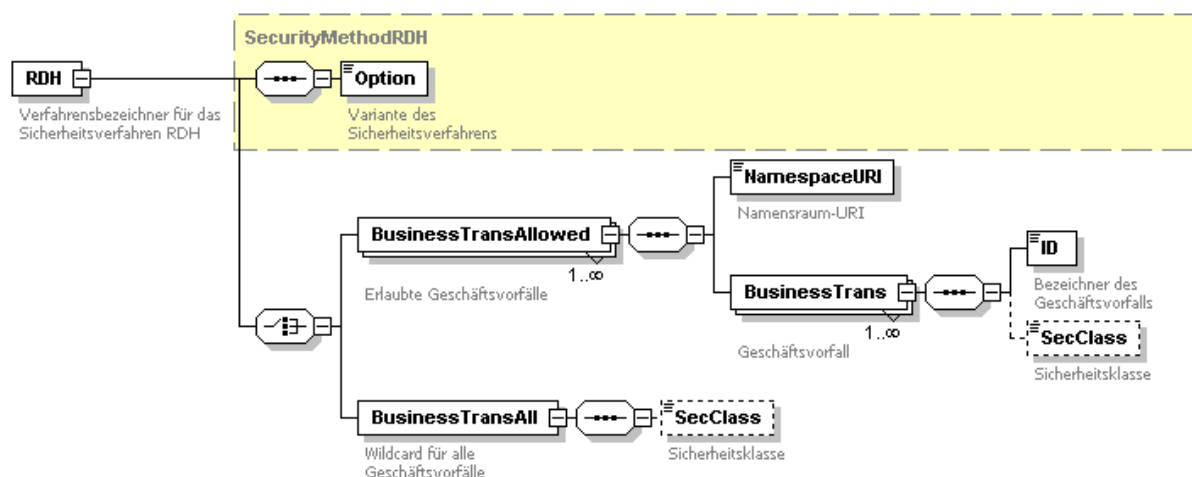


Abbildung 43: Sicherheitsverfahren RDH

Sicherheitsklasse

Bei den Sicherheitsverfahren RDH-3 und RDH-4 ist die Sicherheitsklasse verpflichtend anzugeben. Bei RDH-1 und RDH-2 darf keine Sicherheitsklasse angegeben werden.

| | | |
|--|------------|----------|
| Financial Transaction Services (FinTS) | Version: | Kapitel: |
| Dokument: XML-Syntax | 4.0 | III |
| Kapitel: Nachrichtenaufbau | Stand: | Seite: |
| Abschnitt: Bankparameterdaten | 09.07.2004 | 73 |

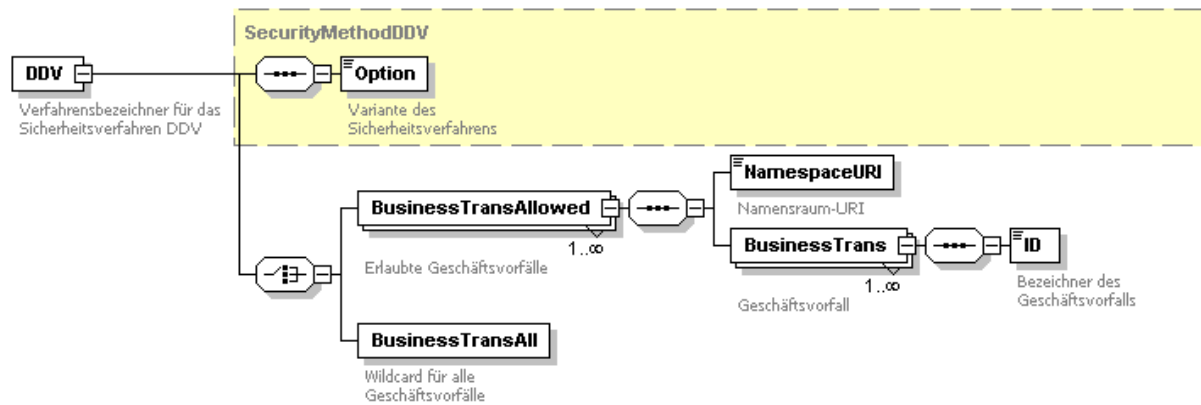


Abbildung 44: Sicherheitsverfahren DDV

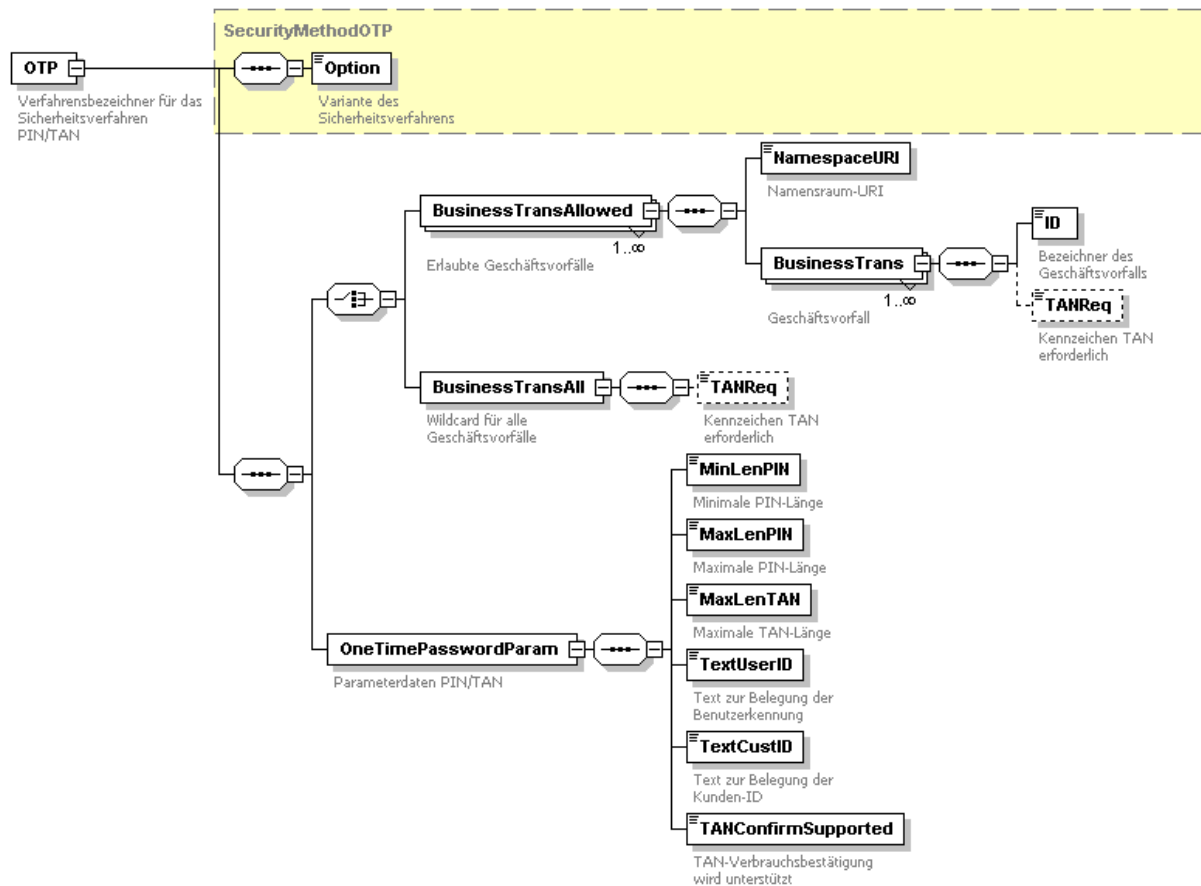


Abbildung 45: Sicherheitsverfahren OneTimePassword

| | | | | |
|----------|-----|------------|--------------------|--|
| Kapitel: | III | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 74 | Stand: | 09.07.2004 | Kapitel: Nachrichtenaufbau |
| | | Abschnitt: | Bankparameterdaten | |

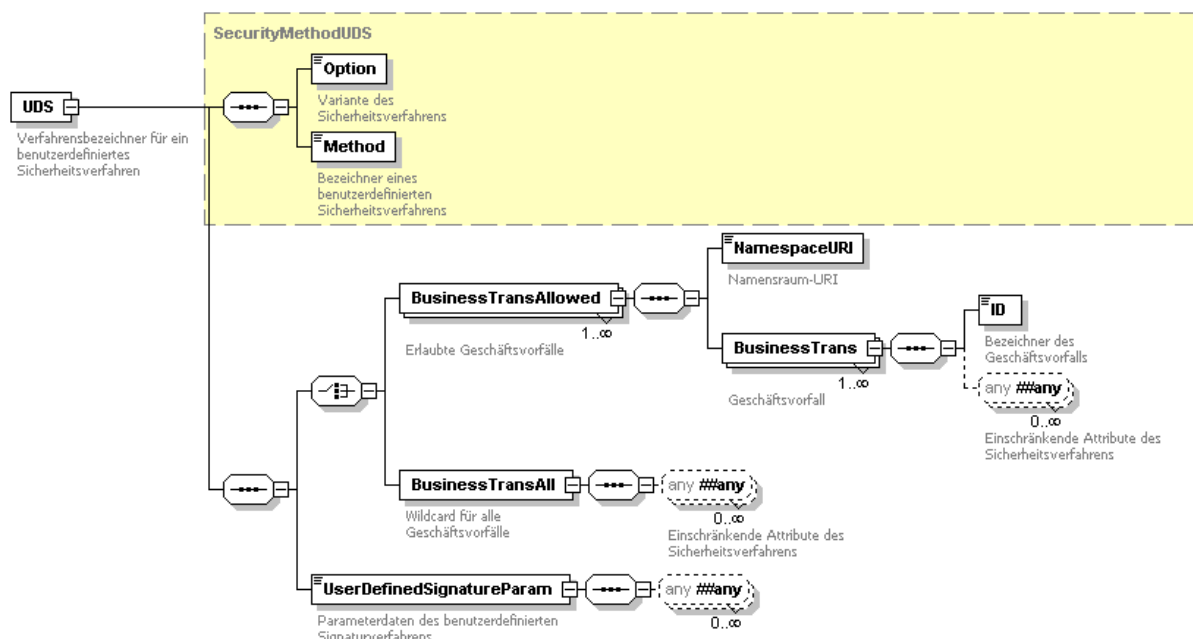


Abbildung 46: Sicherheitsverfahren UserDefinedSignature

d) Komprimierungsverfahren

In diesem Segment gibt das Kreditinstitut die unterstützten Komprimierungsverfahren an.

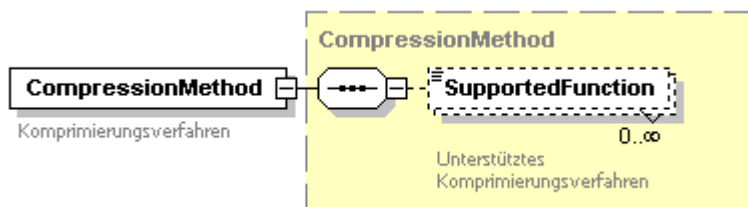


Abbildung 47: Komprimierungsverfahren

e) Geschäftsvorfallparameter

Zu jedem unterstützten Geschäftsvorfall enthalten die BPD ein Parametersegment. Die Anwesenheit oder Abwesenheit dieses Segments legt damit verbindlich fest, ob der Geschäftsvorfall unterstützt wird oder nicht. Wie in II.4 Verbandseigene Geschäftsvorfälle dargestellt, besitzt das Parametersegment eines Geschäftsvorfalles das XML-Tag

`<Name des GV> ' ' <Version des GV> ' ' Par`

und ist im Namensraum des Kundenauftrags- bzw. des Kreditinstitutsantwortsegments definiert.

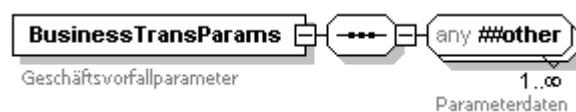


Abbildung 48: Geschäftsvorfallparameter

| | | |
|--|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Bankparameterdaten | Stand: 09.07.2004 | Seite: 75 |

Die Parameterdefinition muss eine Erweiterung des Typs *ParameterData* aus dem Namensraum der FinTS-Typen darstellen und insbesondere dessen allgemeine Elemente *MaxNoOrders* und *MinNoSig* enthalten. Darüber hinaus kann es spezifische Informationen über einen Geschäftsvorfalltyp enthalten.

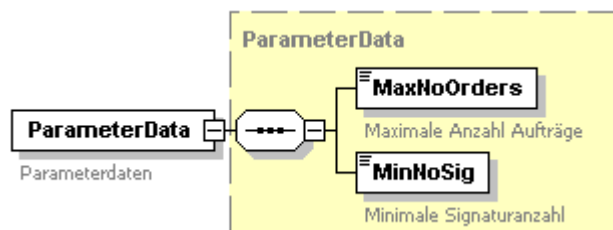


Abbildung 49: Parameterdaten

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 76 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: User-Parameterdaten |

III.6 User-Parameterdaten

In den User-Parameterdaten legt das Kreditinstitut den unterstützten Leistungsumfang für einen bestimmten Benutzer fest und beschreibt diesen durch Parameter (siehe [FORMALS], Abschnitt V. *USER-PARAMETERDATEN (UPD)*). Je nach Kontext kann es sich um die User-Parameterdaten eines Benutzers für den direkten Zugang (UPD), um die User-Parameterdaten eines Benutzers für den Intermediärzugang (UPDI) oder um die User-Parameterdaten eines Intermediärs (IPD) handeln.

Die UPD werden entweder in der Initialisierungsantwort zum Benutzer übertragen oder als Antwort auf einen administrativen Abruf-Auftrag (siehe III.2.2.3 *Initialisierungsantwort*, III.7 *Administrative Aufträge*). Die UPD sind in mehrere Segmente aufgeteilt, die im Folgenden gezeigt werden.

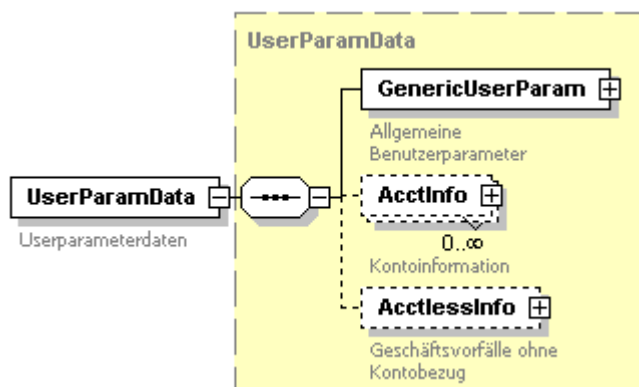


Abbildung 50: User-Parameterdaten

a) Allgemeine Benutzerparameter

Der allgemeine Abschnitt der UPD enthält beschreibende Informationen über die UPD.

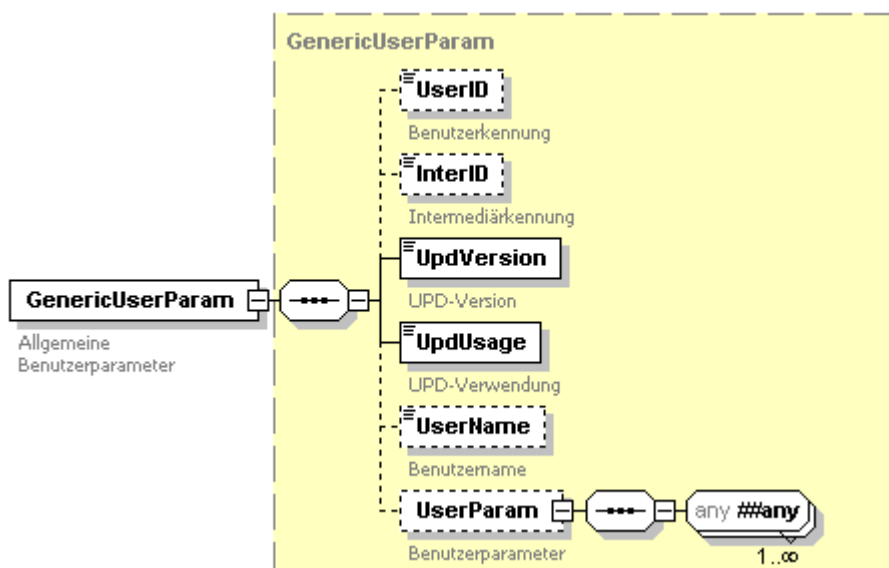


Abbildung 51: Allgemeine UPD

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: User-Parameterdaten | Stand: 09.07.2004 | Seite: 77 |

Benutzerkennung/Intermediärkennung

Handelt es sich um die UPD eines Benutzers, ist die Benutzerkennung belegt. Handelt es sich um die IPD eines Intermediärs, ist die Intermediärkennung belegt. In den UPD eines Benutzers für einen Intermediärzugang (UPDI) sind beide Kennungen belegt. Bei UPD für den anonymen Zugang (Gast-UPD) fehlen beide Kennungen.

b) Kontoinformation

Zu jedem Konto des Benutzers ist in den UPD ein Segment Kontoinformation hinterlegt. Es enthält Details zum Konto sowie eine Liste der für dieses Konto erlaubten Geschäftsvorfalltypen und optional ein kontospezifisches Limit. Bei UPD für den anonymen Zugang sowie bei IPD sind keine Segmente mit Kontobezug vorhanden.

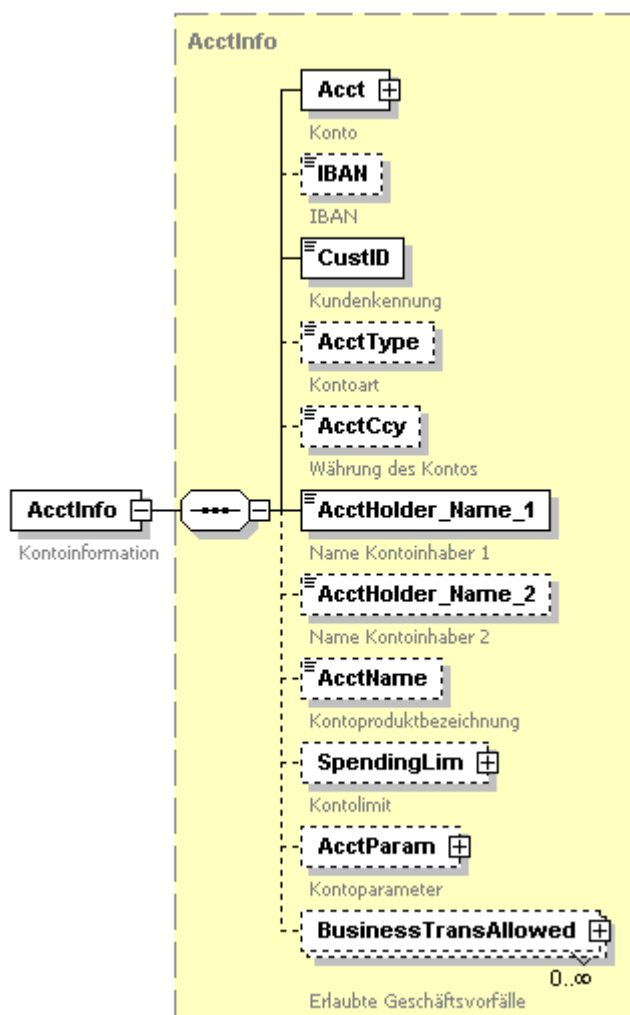


Abbildung 52: Kontoinformationen

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 78 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: User-Parameterdaten |

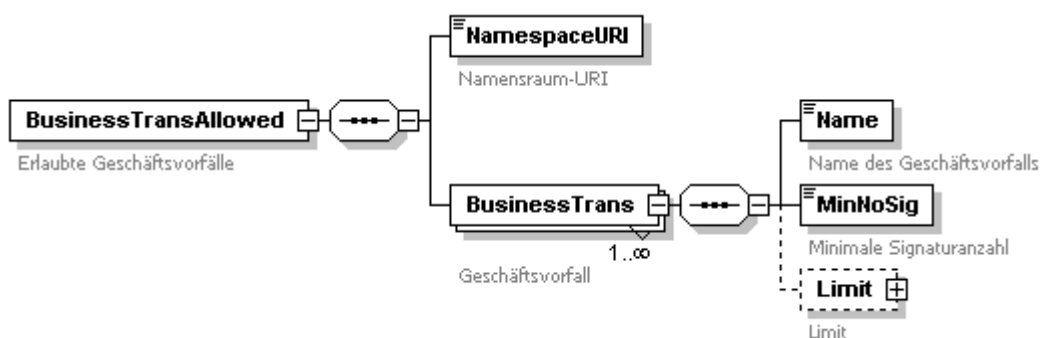


Abbildung 53: Erlaubte Geschäftsvorfälle

c) Geschäftsvorfälle ohne Kontobezug

Alle Geschäftsvorfälle, die im Auftrag keinen Bezug zu einem Konto aufweisen, werden in den UPD in einem eigenen Segment gruppiert. Sie sind auf jedem Konto zulässig. Die Geschäftsvorfall-Einträge in den *AcctInfo* und *AcctlessInfo*-Elementen sollten sich nicht überschneiden. Bei UPD für den anonymen Zugang sowie bei IPD ist nur dieses Segment belegt, Geschäftsvorfälle mit Kontobezug gibt es in diesen Fällen nicht.

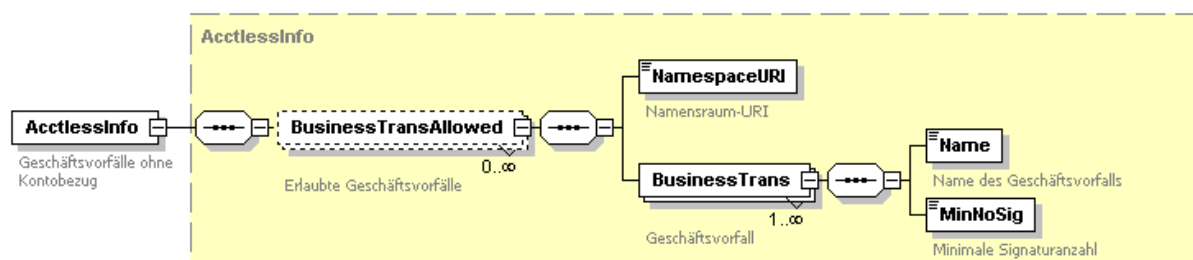


Abbildung 54: Geschäftsvorfälle ohne Kontobezug

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 79 |

III.7 Administrative Aufträge

Dieser Abschnitt beschreibt die administrativen Aufträge in FinTS. Dieses sind die Anforderungen von BPD, UPD, IPD und UPDI, Aufträge für Intermediärszenarien, die PIN/TAN-Aufträge, Aufträge in Zusammenhang mit dem Abonnement, der Adressenregistrierung, verteilten Signaturen, der Quittung und dem Statusprotokoll. Alle diese Aufträge werden in Standard-Benutzernachrichten eingestellt.

Die Beschreibung eines Auftrags gliedert sich jeweils in die Abschnitte Benutzerauftrag, Kreditinstitutsrückmeldung und Bankparameterdaten (die Geschäftsvorfallparameter zu diesem Auftrag). Zu den enthaltenen Elementen sind Texte zur Belegung unter den Abbildungen enthalten, wenn sie nicht der Standardbedeutung aus dem [DataDictionary] entsprechen.

Die Bankparameterdaten enthalten jeweils mindestens die Felder zur minimal erforderlichen Anzahl der Signaturen und maximalen Anzahl möglicher Aufträge.

In einem ersten Abschnitt werden zunächst allgemeine Typen beschrieben. Darauf folgend sind die administrativen Aufträge beschrieben.

III.7.1 BPD

Neben der Möglichkeit, BPD als Teil der Initialisierungsantwort zu erhalten, können BPD mit einem administrativen Auftrag angefordert werden. Dies ist insbesondere in Intermediärszenarien von Bedeutung.

III.7.1.1 BPD anfordern

Mit diesem Auftrag fordert ein Benutzer die Bankparameterdaten eines Kreditinstituts an (siehe [Formals], Abschnitt IV.3 Anforderung der BPD in einem Szenario mit Intermediär).

a) Benutzerauftrag

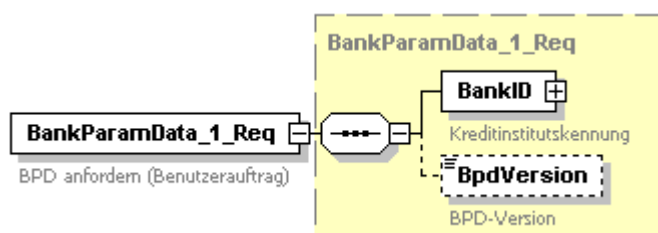


Abbildung 55: Benutzerauftrag BPD anfordern

BPD-Version

Falls die BPD-Version angegeben wird, wird die BPD nur geliefert, wenn sie neuer ist. Andernfalls wird immer die aktuelle BPD geliefert.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 80 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

b) Kreditinstitutsrückmeldung

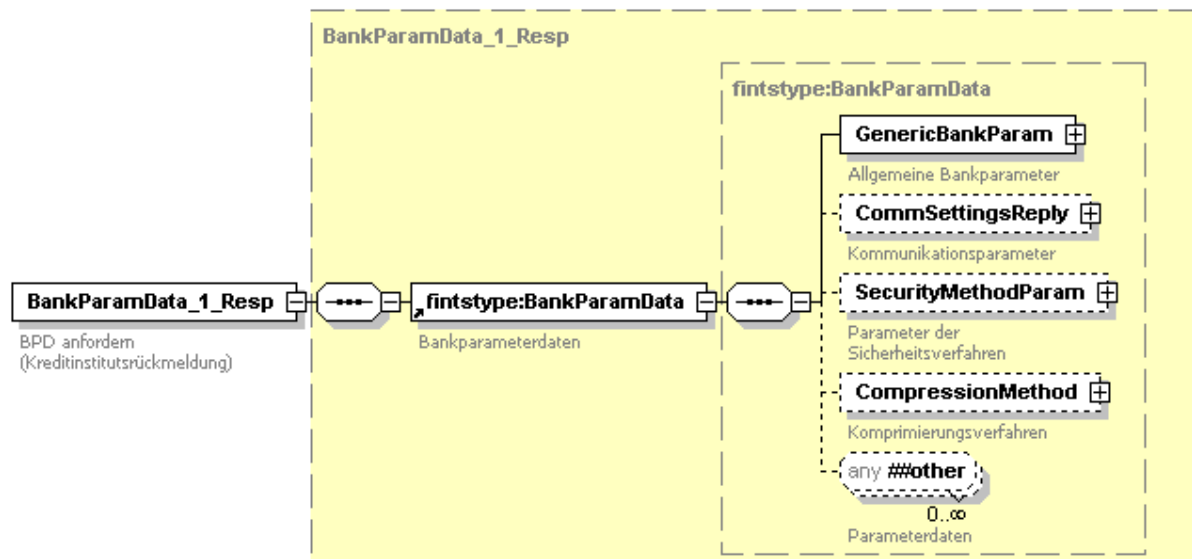


Abbildung 56: Kreditinstitutsrückmeldung BPD anfordern

c) Bankparameterdaten

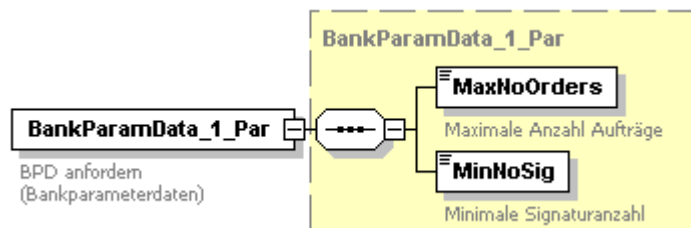


Abbildung 57: Bankparameterdaten BPD anfordern

III.7.2 UPD

Neben der Möglichkeit, UPD als Teil der Initialisierungsantwort zu erhalten, können UPD mit einem administrativen Auftrag angefordert werden. Dies ist insbesondere in Intermediärszenarien von Bedeutung. In diesen Szenarien sind außer den normalen UPD des Benutzers auch UPD des Intermediärs (IPD) und intermediärbezogene UPD des Benutzers (UPDI) definiert, welche ebenfalls mit diesem Auftrag abgeholt werden können.

III.7.2.1 UPD anfordern

Mit diesem Auftrag könne die UPD, IPD oder UPDI angefordert werden (siehe [Formals], Abschnitt *V.6 Explizite Anforderung von UPD*).

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 81 |

a) Benutzerauftrag

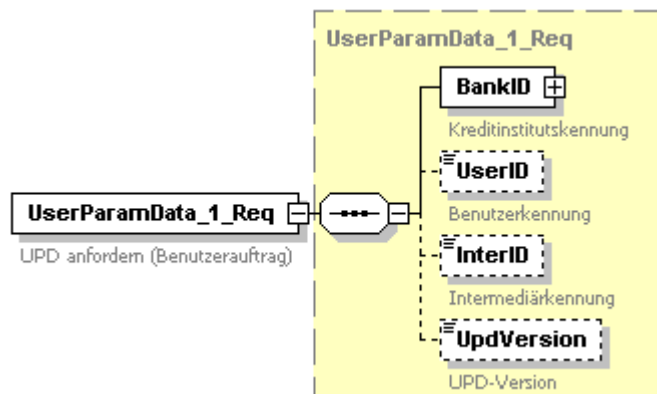


Abbildung 58: Benutzerauftrag UPD anfordern

Benutzerkennung/Intermediärkennung

Bei Anforderung der User-Parameterdaten eines Benutzers für den direkten Zugang (UPD) ist die Benutzerkennung anzugeben. Bei Anforderung der User-Parameterdaten eines Intermediärs (IPD) ist die Intermediärkennung anzugeben. Bei Anforderung der User-Parameterdaten eines Benutzers für einen Intermediärzugang (UPDI) sind beide Kennungen anzugeben. Bei Anforderung der UPD für den anonymen Zugang (Gast-UPD) ist keine der Kennungen anzugeben.

UPD-Version

Falls die UPD-Version angegeben wird, wird die UPD nur geliefert wenn sie neuer ist. Andernfalls wird immer die aktuelle UPD geliefert.

b) Kreditinstitutsrückmeldung

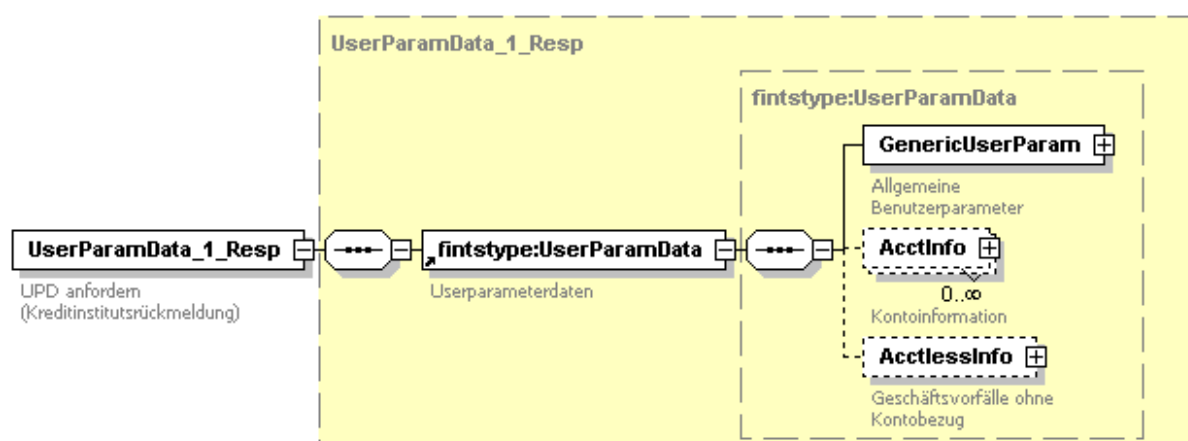


Abbildung 59: Kreditinstitutsrückmeldung UPD anfordern

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 82 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

c) Bankparameterdaten

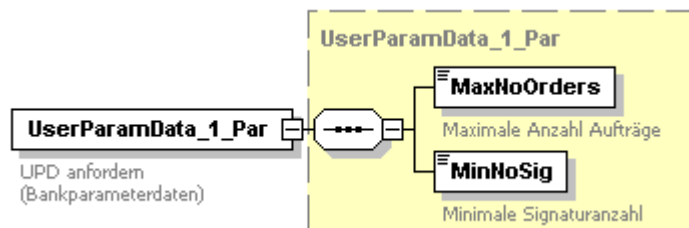


Abbildung 60: Bankparameterdaten UPD anfordern

III.7.3 Intermediärszenarien

Für die Kommunikation über einen Intermediär sind administrative Geschäftsvorfälle definiert, die zur Verwaltung der Intermediärbenutzung durch das Kreditinstitut dienen.

III.7.3.1 Liste der Intermediäre

Mit diesem Auftrag kann der Benutzer Informationen über Intermediäre abrufen (siehe [Formals], Abschnitt V.7 *Pflege der Intermediärzugänge und der UPDI*).

a) Benutzerauftrag



Abbildung 61: Benutzerauftrag Liste der Intermediäre

b) Kreditinstitutsrückmeldung

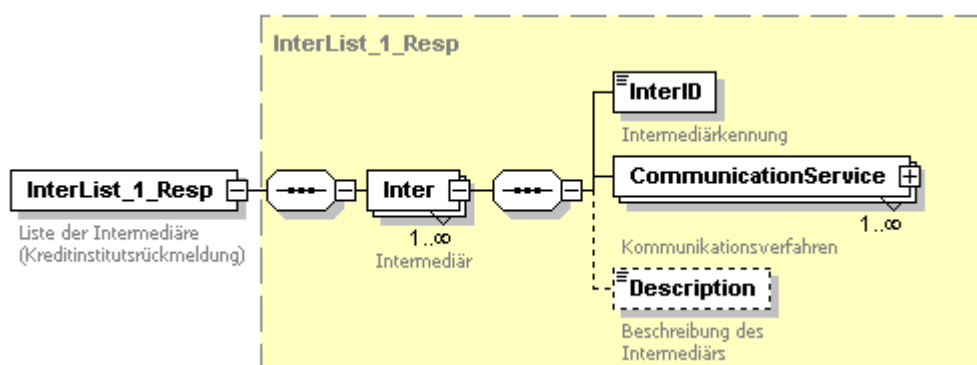


Abbildung 62: Kreditinstitutsrückmeldung Liste der Intermediäre

Beschreibung des Intermediärs

Hier kann eine textuelle Beschreibung des Intermediärs angegeben werden.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 83 |

c) Bankparameterdaten

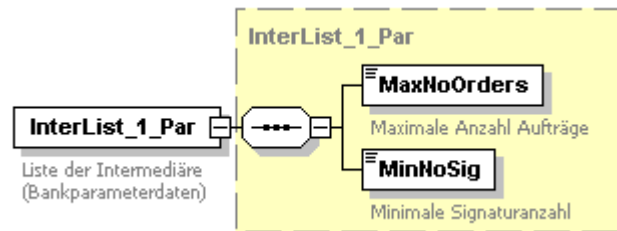


Abbildung 63: Bankparameterdaten Liste der Intermediäre

III.7.3.2 Für einen Intermediär anmelden

Mit diesem Auftrag kann ein Benutzer sich für die Benutzung bei einem Intermediär anmelden (siehe [Formals], Abschnitt V.7 *Pflege der Intermediärzugänge und der UPDI*).

a) Benutzerauftrag

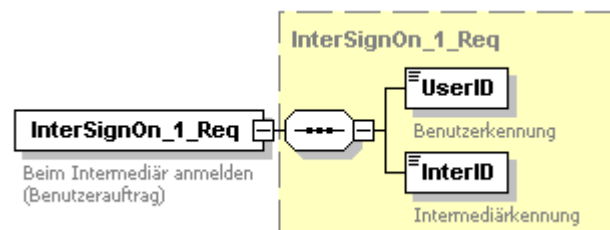


Abbildung 64: Benutzerauftrag Für einen Intermediär anmelden

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

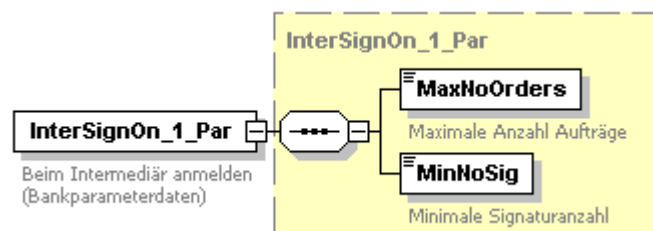


Abbildung 65: Bankparameterdaten Für einen Intermediär anmelden

III.7.3.3 Für einen Intermediär abmelden

Mit diesem Auftrag kann ein Benutzer sich für die Benutzung bei einem Intermediär abmelden (siehe [Formals], Abschnitt V.7 *Pflege der Intermediärzugänge und der UPDI*).

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 84 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

a) Benutzerauftrag

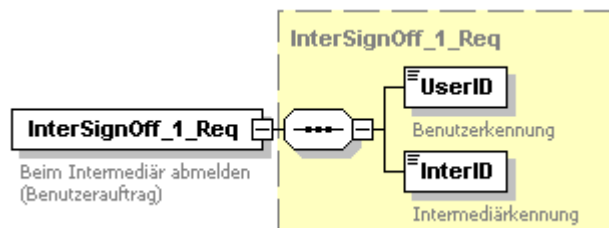


Abbildung 66: Benutzerauftrag Für einen Intermediär abmelden

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

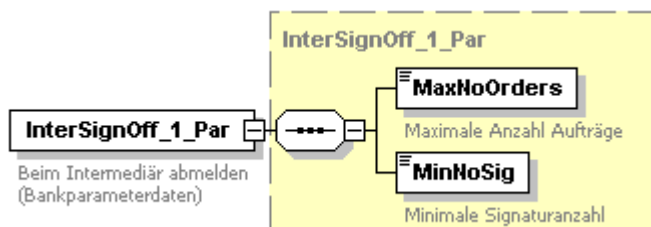


Abbildung 67: Bankparameterdaten Für einen Intermediär abmelden

III.7.3.4 UPDI ändern

Mit diesem Auftrag kann der Benutzer geänderte UPDI beim Kreditinstitut einreichen (siehe [Formals], Abschnitt V.7 *Pflege der Intermediärzugänge und der UPDI*).

a) Benutzerauftrag

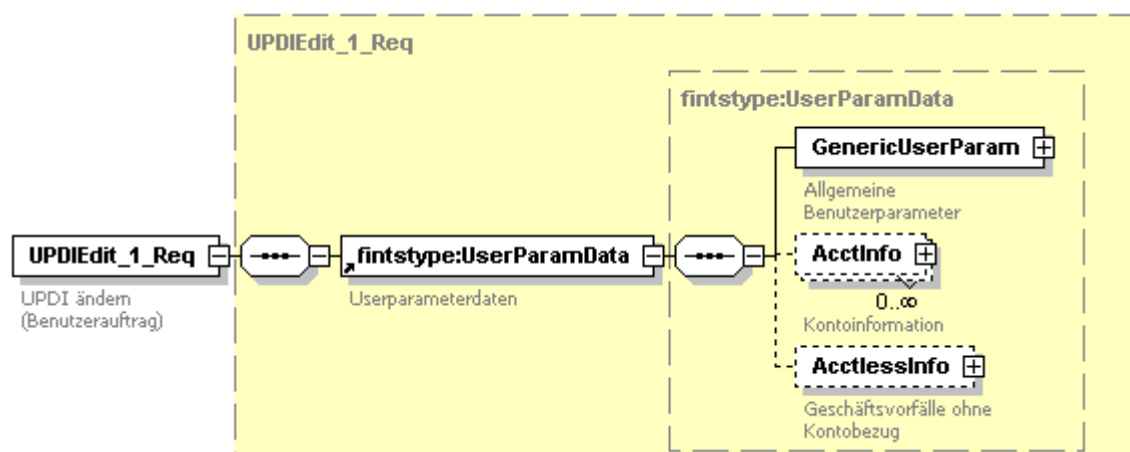


Abbildung 68: Benutzerauftrag UPDI ändern

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 85 |

c) Bankparameterdaten

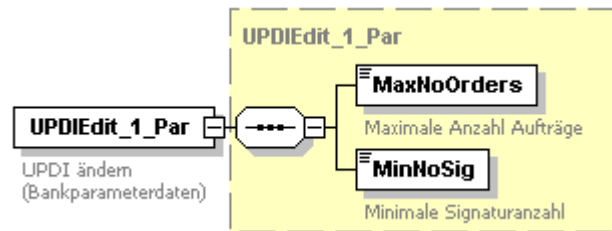


Abbildung 69: Bankparameterdaten UPDI ändern

III.7.4 PIN/TAN

Im Sicherheitsverfahren PIN/TAN werden administrative Geschäftsvorfälle zur Verwaltung der TAN-Listen und der PIN benötigt.

III.7.4.1 PIN ändern

Mit diesem Auftrag kann ein Benutzer seine PIN ändern (siehe [PINTAN], Abschnitt II.6.1.1 PIN-Änderung).

a) Benutzerauftrag

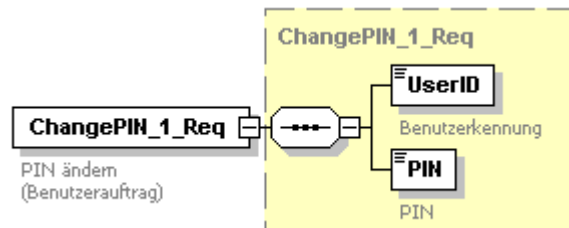


Abbildung 70: Benutzerauftrag PIN ändern

PIN

Hier ist die neu einzurichtende PIN anzugeben.

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

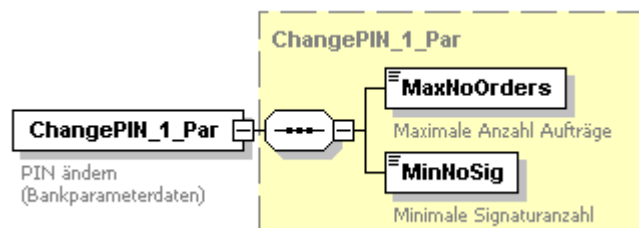


Abbildung 71: Bankparameterdaten PIN ändern

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 86 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

III.7.4.2 TAN-Liste anfordern

Mit diesem Auftrag kann ein Benutzer eine TAN-Liste anfordern (siehe [PINTAN], Abschnitt II.6.1.2 TAN-Liste anfordern).

a) Benutzerauftrag

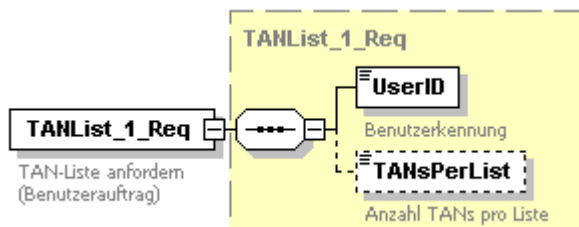


Abbildung 72: Benutzerauftrag TAN-Liste anfordern

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

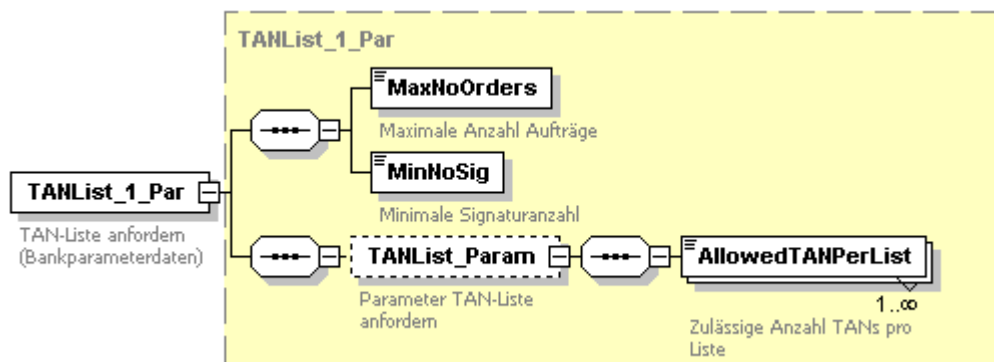


Abbildung 73: Bankparameterdaten TAN-Liste anfordern

III.7.4.3 TAN-Liste freischalten

Mit diesem Auftrag kann ein Benutzer eine TAN-Liste freischalten (siehe [PINTAN], Abschnitt II.6.1.3 TAN-Liste freischalten).

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 87 |

a) Benutzerauftrag

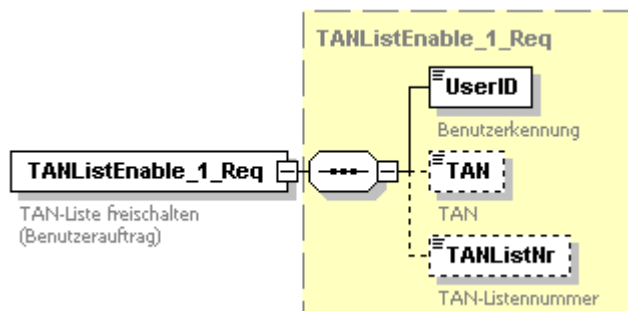


Abbildung 74: Benutzerauftrag TAN-Liste freischalten

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

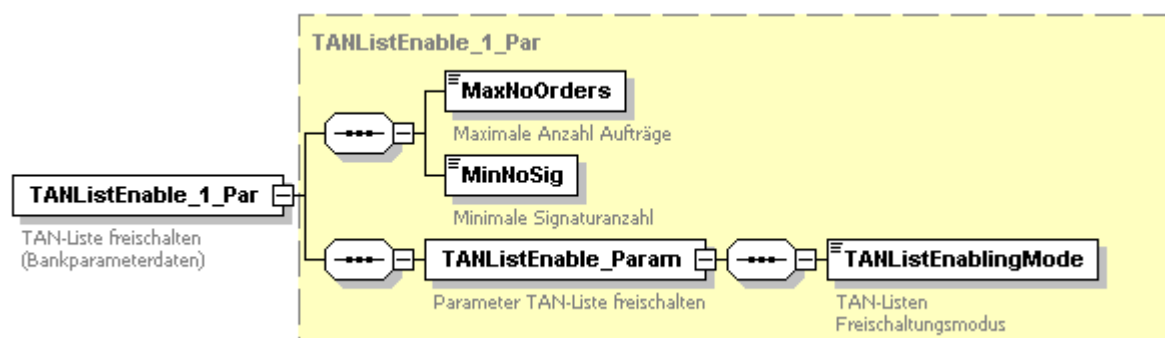


Abbildung 75: Bankparameterdaten TAN-Liste freischalten

III.7.4.4 PIN sperren

Mit diesem Auftrag kann ein Benutzer seine PIN sperren (siehe [PINTAN], Abschnitt II.6.2.2 PIN-Sperre).

a) Benutzerauftrag

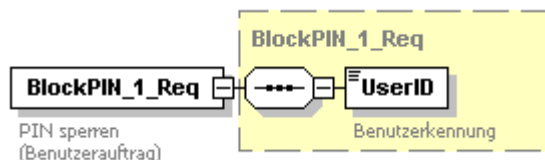


Abbildung 76: Benutzerauftrag PIN-Sperre

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 88 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

c) Bankparameterdaten

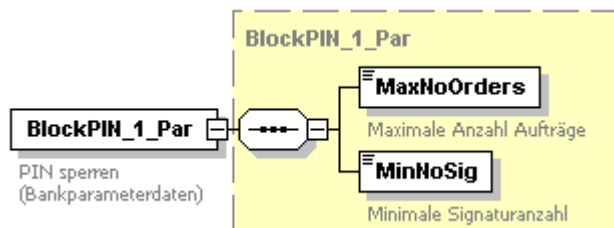


Abbildung 77: Bankparameterdaten PIN-Sperre

III.7.4.5 PIN-Sperre aufheben

Mit diesem Auftrag kann ein Benutzer eine PIN-Sperre aufheben (siehe [PINTAN], Abschnitt II.6.2.3 PIN-Sperre aufheben).

a) Benutzerauftrag

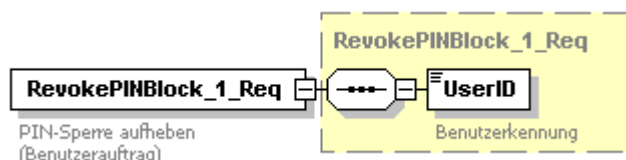


Abbildung 78: Benutzerauftrag PIN-Sperre aufheben

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

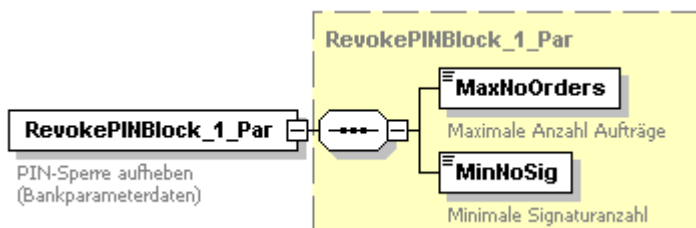


Abbildung 79: Bankparameterdaten PIN-Sperre aufheben

III.7.4.6 TAN-Liste sperren/löschen

Mit diesem Auftrag kann ein Benutzer eine TAN-Liste sperren (siehe [PINTAN], Abschnitt II.6.2.4 TAN-Liste sperren/löschen).

a) Benutzerauftrag

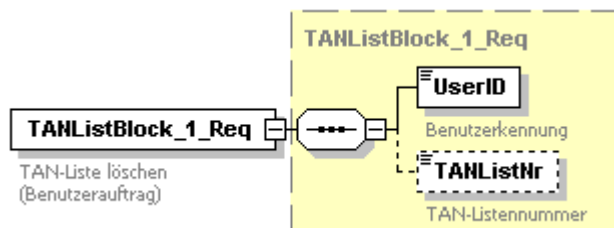


Abbildung 80: Benutzerauftrag TAN-Liste sperren/löschen

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

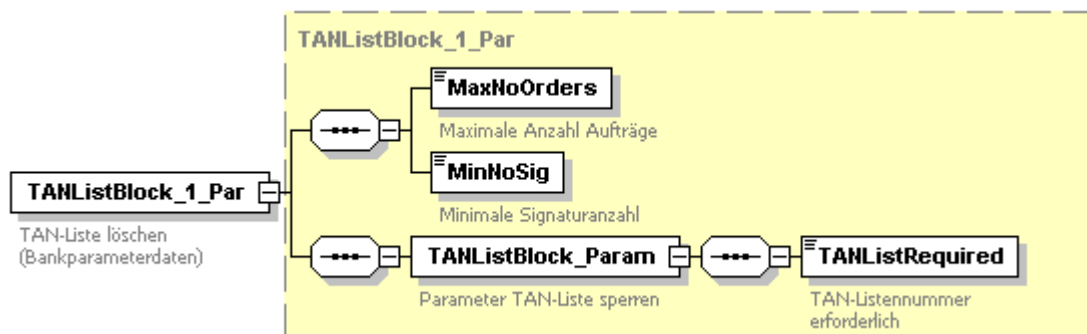


Abbildung 81: Bankparameterdaten TAN-Liste sperren/löschen

III.7.4.7 TAN-Verbrauchsinformationen anfordern

Mit diesem Auftrag kann ein Benutzer sich anzeigen lassen, welche TANs einer Liste er verbraucht hat (siehe [PINTAN], Abschnitt II.6.3.1 TAN-Verbrauchsinformationen anzeigen).

a) Benutzerauftrag

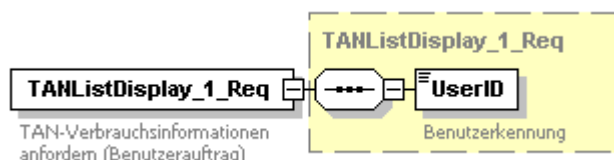


Abbildung 82: Benutzerauftrag TAN-Verbrauchsinformationen anfordern

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 90 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

b) Kreditinstitutsrückmeldung

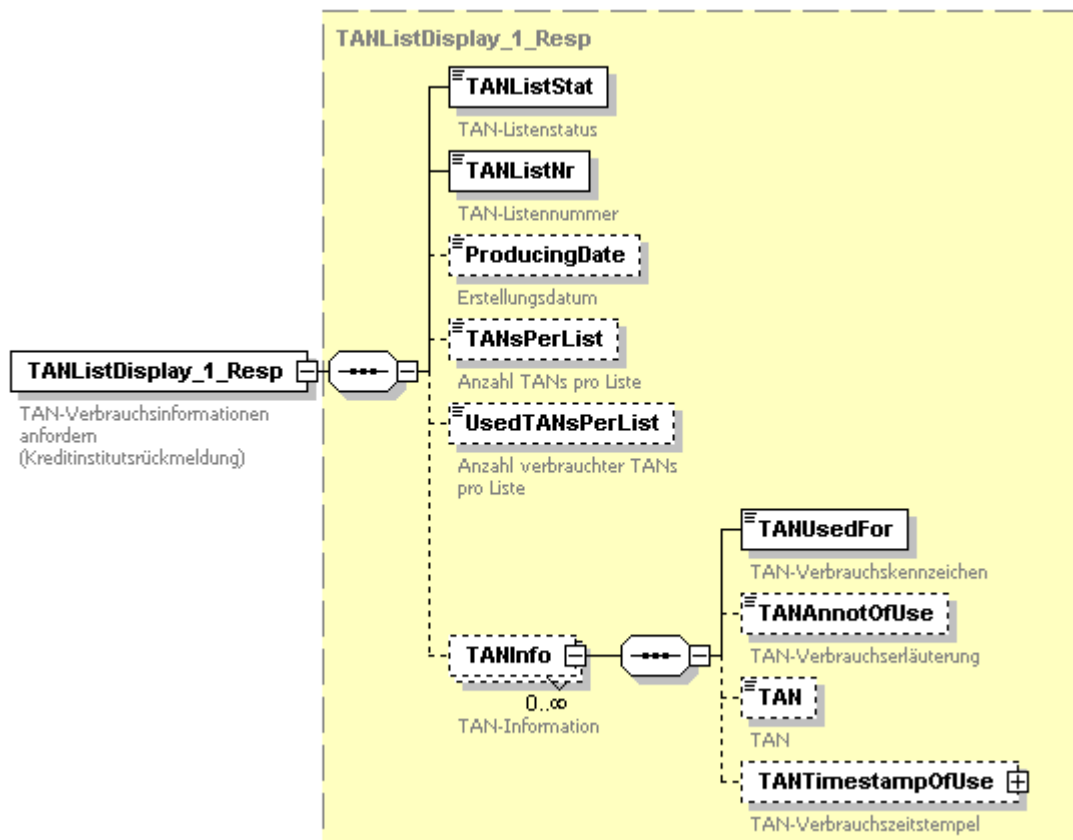


Abbildung 83: Kreditinstitutsrückmeldung TAN-Verbrauchsinformationen anfordern

c) Bankparameterdaten

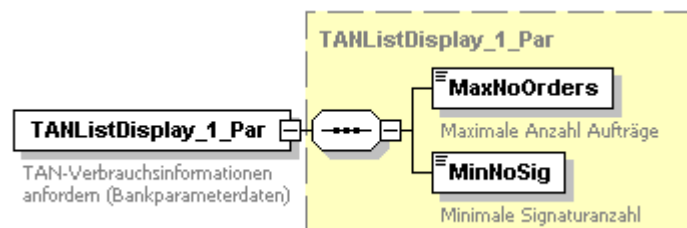


Abbildung 84: Bankparameterdaten TAN-Verbrauchsinformationen anfordern

III.7.5 Abonnement

III.7.5.1 Abonnement einreichen

Mit diesem Auftrag kann ein Benutzer eine Subscription (Abonnement) einrichten (siehe [Formals], Abschnitt III.7 Das Publish/Subscribe-Verfahren).

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 91 |

a) Benutzerauftrag

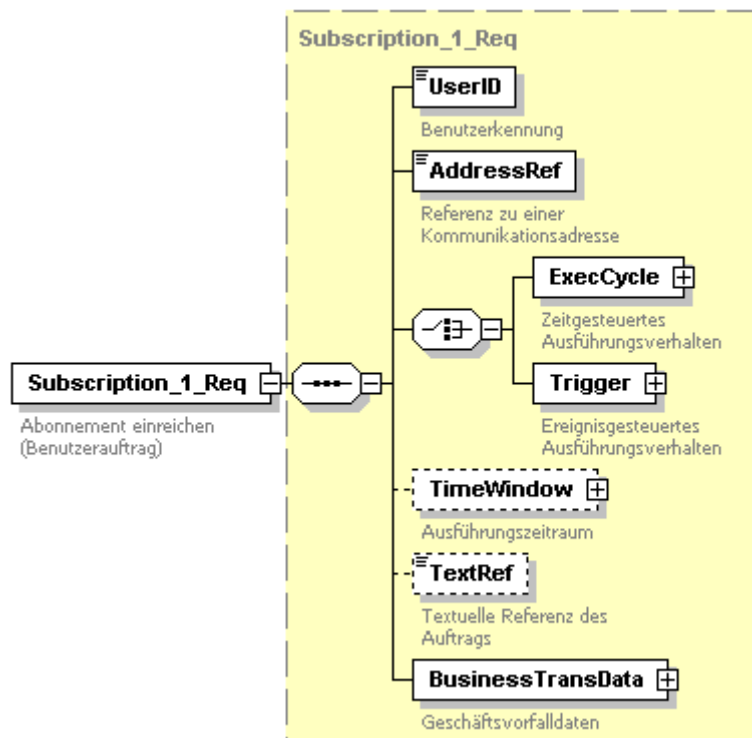


Abbildung 85: Benutzerauftrag Abonnement einreichen

b) Kreditinstitutsrückmeldung

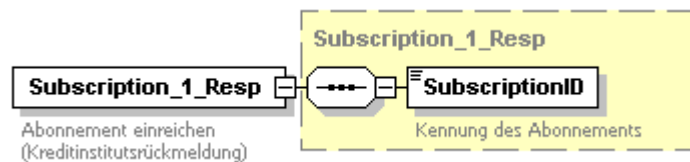


Abbildung 86: Kreditinstitutsrückmeldung Abonnement einreichen

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 92 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

c) Bankparameterdaten

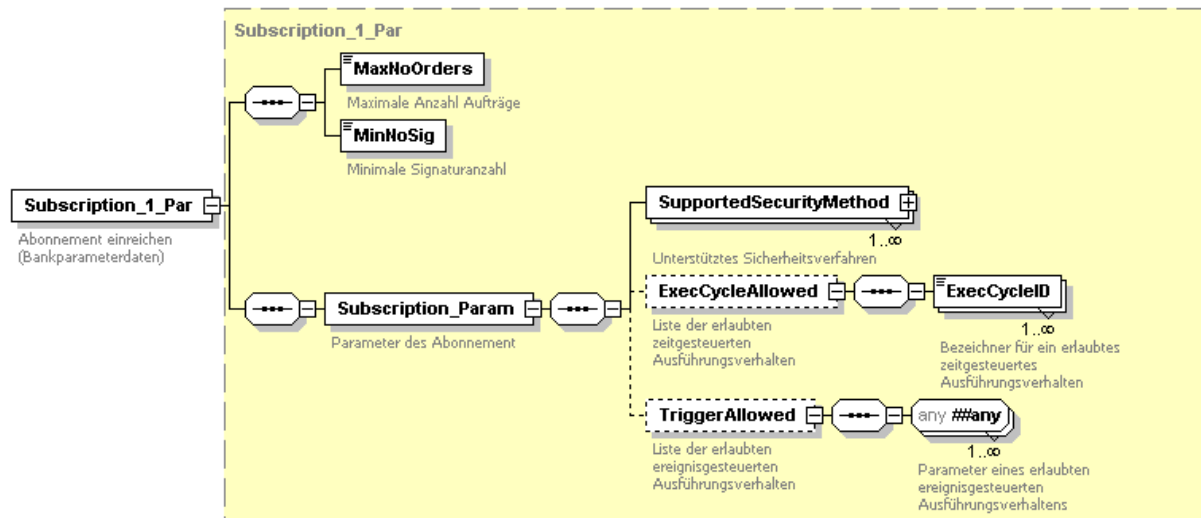


Abbildung 87: Bankparameterdaten Abonnement einreichen

Die Parameter dieses Geschäftsvorfalles enthalten insbesondere die Liste, der in einem bestimmten Sicherheitsverfahren abonmierbaren Geschäftsvorfälle, in den Elementen *SupportedSecurityMethod*:

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 93 |

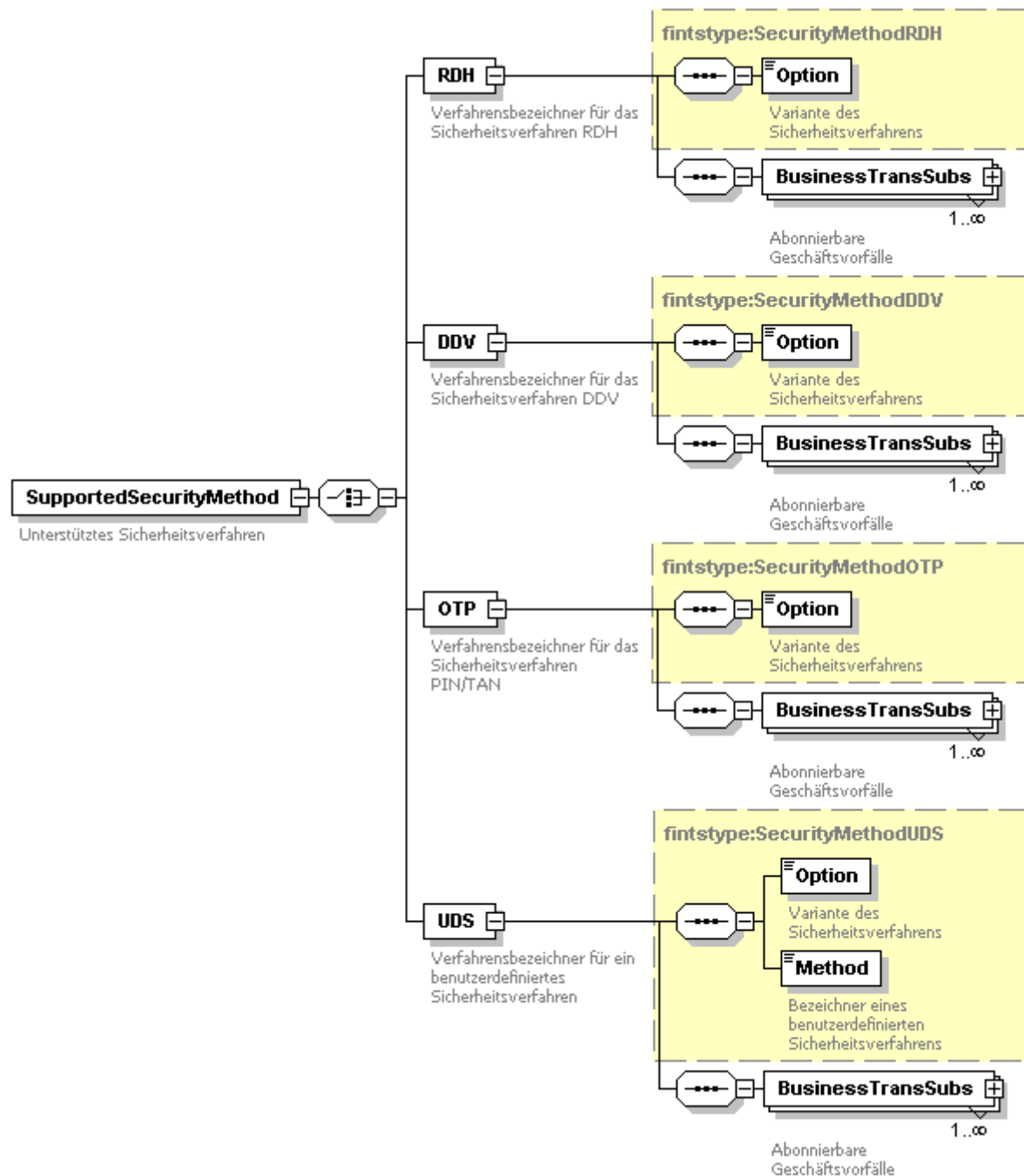


Abbildung 88: Unterstützte Sicherheitsverfahren

III.7.5.2 Abonnement löschen

Mit diesem Auftrag kann ein Benutzer ein Abonnement löschen (siehe [Formals], Abschnitt III.7 Das Publish/Subscribe-Verfahren).

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 94 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

a) Benutzerauftrag

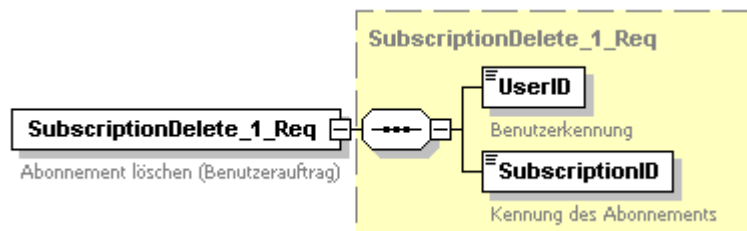


Abbildung 89: Benutzerauftrag Abonnement löschen

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

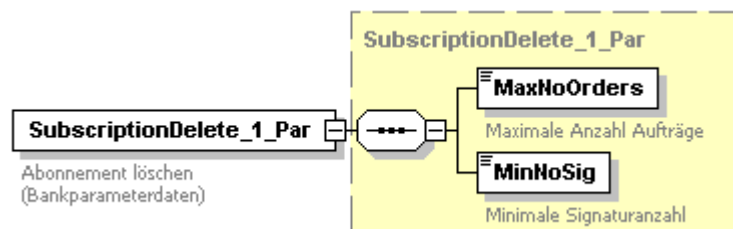


Abbildung 90: Bankparameterdaten Abonnement löschen

III.7.5.3 Abonnementsinformationen anfordern

Mit diesem Auftrag kann ein Benutzer Informationen über Abonnements abrufen (siehe [Formals], Abschnitt III.7 Das Publish/Subscribe-Verfahren).

a) Benutzerauftrag

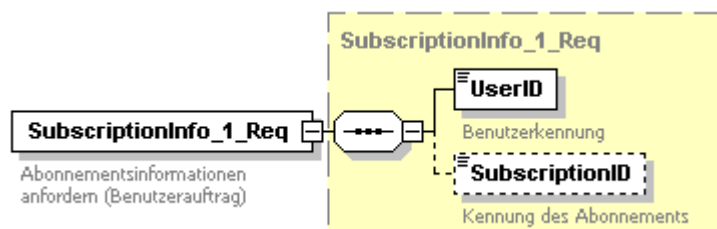


Abbildung 91: Benutzerauftrag Abonnementsinformationen anfordern

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 95 |

b) Kreditinstitutsrückmeldung

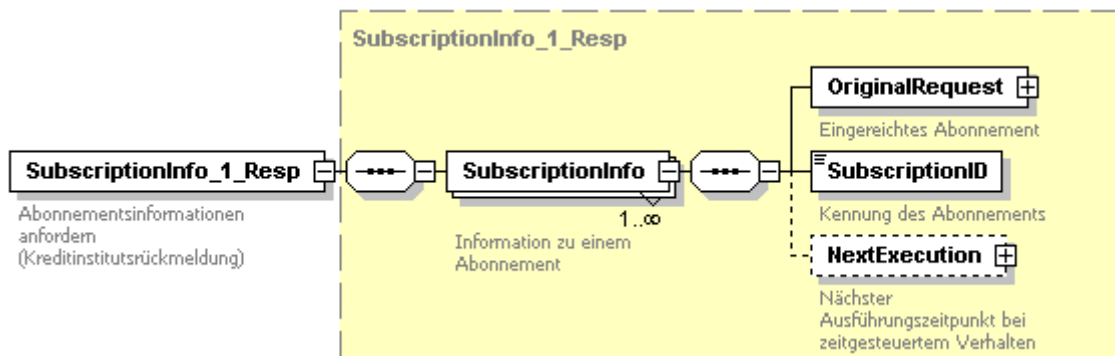


Abbildung 92: Kreditinstitutsrückmeldung Abonnementsinformationen anfordern

c) Bankparameterdaten

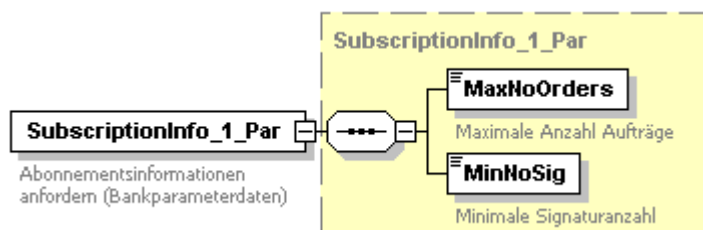


Abbildung 93: Bankparameterdaten Abonnementsinformationen anfordern

III.7.6 Adressenregistrierung

Für asynchrone Kommunikation werden Adressen des Benutzers verwendet, die dieser mit den hier aufgeführten Geschäftsvorfällen registrieren und verwalten kann.

III.7.6.1 Adresse registrieren

Mit diesem Auftrag kann ein Benutzer eine Adresse registrieren (siehe [Formals], Abschnitt *III.4 Adressregistrierung*)

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 96 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

a) Benutzerauftrag

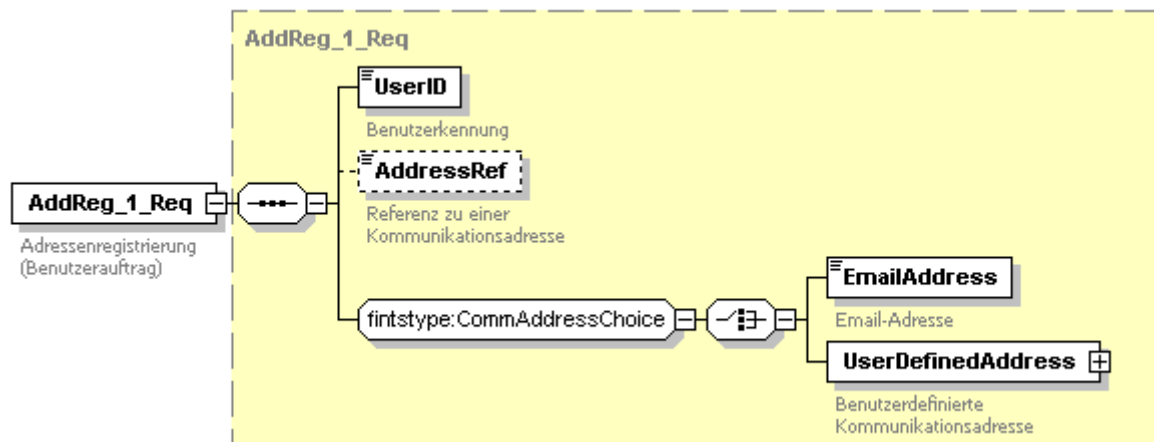


Abbildung 94: Benutzerauftrag Adresse registrieren

b) Kreditinstitutsrückmeldung

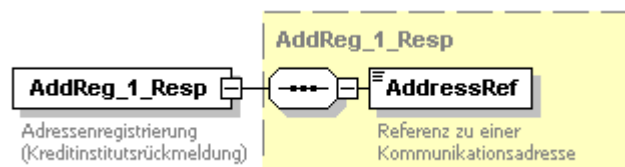


Abbildung 95: Kreditinstitutsrückmeldung Adresse registrieren

c) Bankparameterdaten

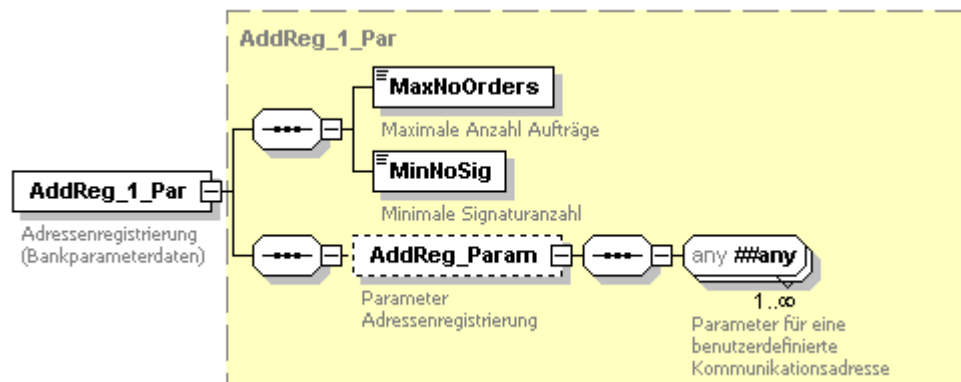


Abbildung 96: Bankparameterdaten Adresse registrieren

III.7.6.2 Adressregistrierungsinformationen holen

Mit diesem Auftrag kann ein Benutzer sich die Adressinformationen geben lassen (siehe [Formals], Abschnitt III.4 Adressregistrierung).

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 97 |

a) Benutzerauftrag

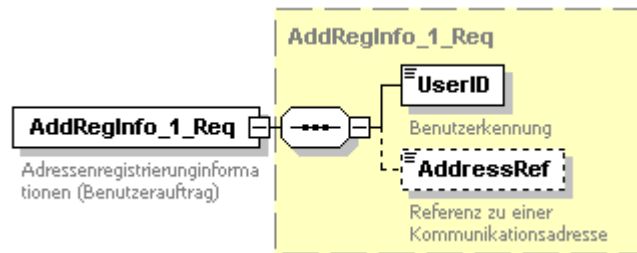


Abbildung 97: Benutzerauftrag Adressregistrierungsinformationen holen

b) Kreditinstitutsrückmeldung

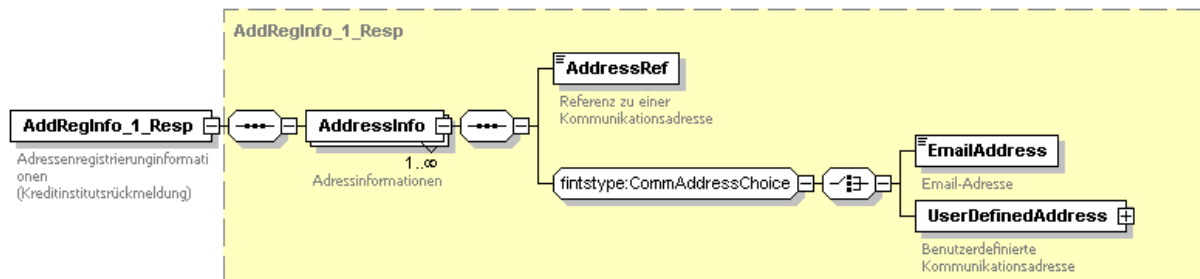


Abbildung 98: Kreditinstitutsrückmeldung Adressregistrierungsinformationen holen

c) Bankparameterdaten

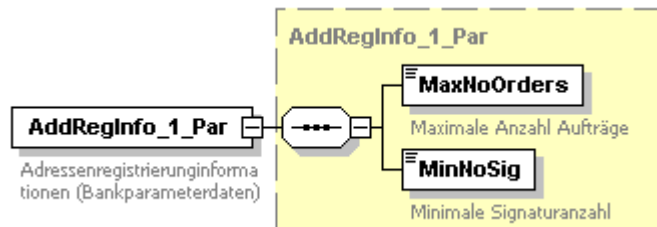


Abbildung 99: Bankparameterdaten Adressregistrierungsinformationen holen

III.7.6.3 Adressregistrierung löschen

Mit diesem Auftrag kann ein Benutzer die Adressinformationen löschen (siehe [Formals], Abschnitt III.4 Adressregistrierung).

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 98 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

a) Benutzerauftrag

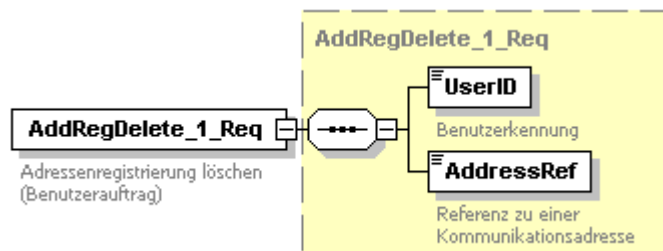


Abbildung 100: Benutzerauftrag Adressregistrierung löschen

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

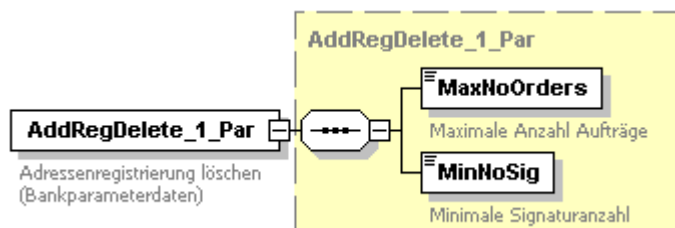


Abbildung 101: Bankparameterdaten Adressregistrierung löschen

III.7.7 Quittung

Für bestimmte Aufträge kann ein Quittierungsverfahren vorgeschrieben sein, der Erhalt der Kreditinstitutsnachricht muss dann mit dem hier gezeigten administrativen Auftrag bestätigt werden.

III.7.7.1 Quittung

Mit diesem Auftrag bestätigt ein Benutzer den Erhalt einer Antwort (siehe [Formals], Abschnitt III.5 Quittierung von Aufträgen).

a) Benutzerauftrag

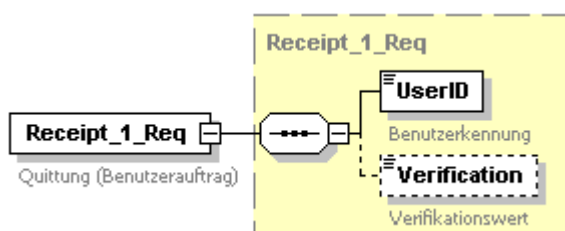


Abbildung 102: Benutzerauftrag Quittung

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

| | | |
|--|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 99 |

c) Bankparameterdaten

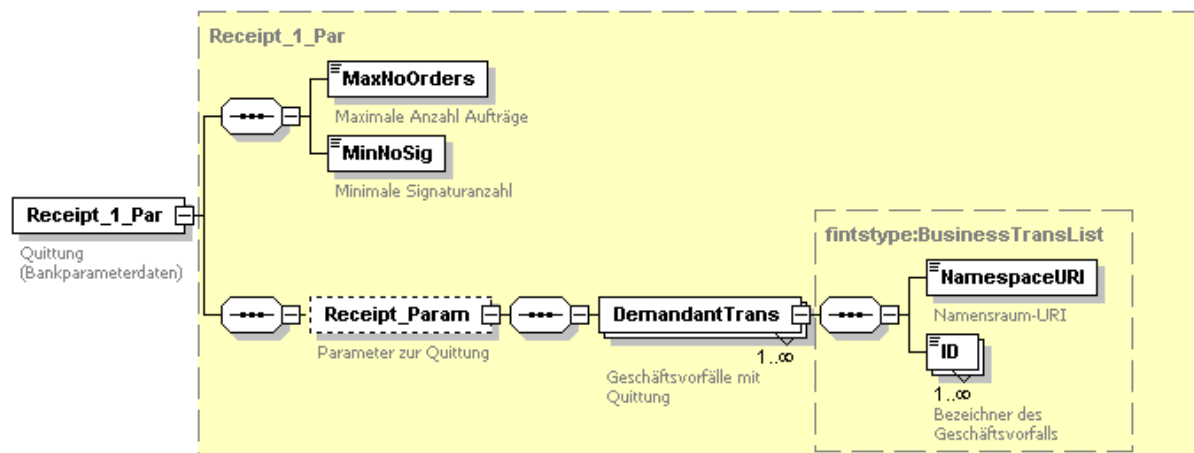


Abbildung 103: Bankparameterdaten Quittung

III.7.8 Verteile Signaturen

Das Verfahren zu verteilten Signaturen ermöglicht es, einen Auftrag beim Kreditinstitut lagern zu lassen und die benötigten Signaturen sukzessive nachzureichen, bis der Auftrag schließlich verarbeitungsfähig ist.

III.7.8.1 Auftrag mit verteilten Signaturen einreichen

Mit diesem Auftrag kann ein Benutzer einen Auftrag einreichen, der später noch von anderen Benutzern signiert werden muss (siehe [Formals], Abschnitt *III.8 Verteilte Signaturen*).

a) Benutzerauftrag

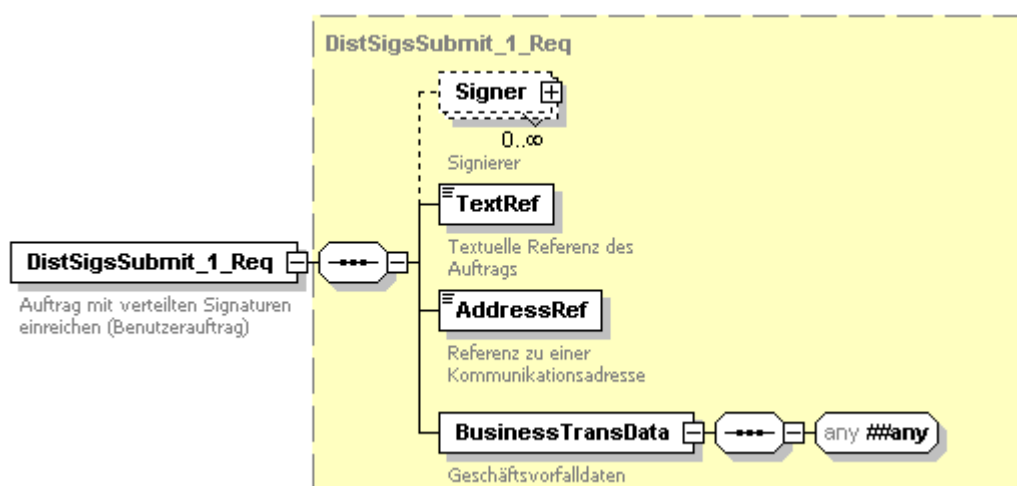


Abbildung 104: Benutzerauftrag Auftrag mit verteilten Signaturen einreichen

Signierer

Wenn die Liste der Signierenden vorhanden ist, wird ihre Interpretation durch eine bilaterale Vereinbarung zwischen Kreditinstitut und Benutzer festgelegt. Ansonsten legt das Kreditinstitut die Signierenden fest.

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 100 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

b) Kreditinstitutsrückmeldung

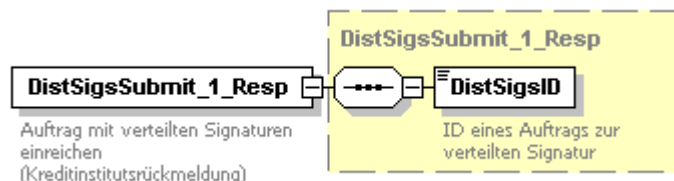


Abbildung 105: Kreditinstitutsrückmeldung Auftrag mit verteilten Signaturen einreichen

c) Bankparameterdaten

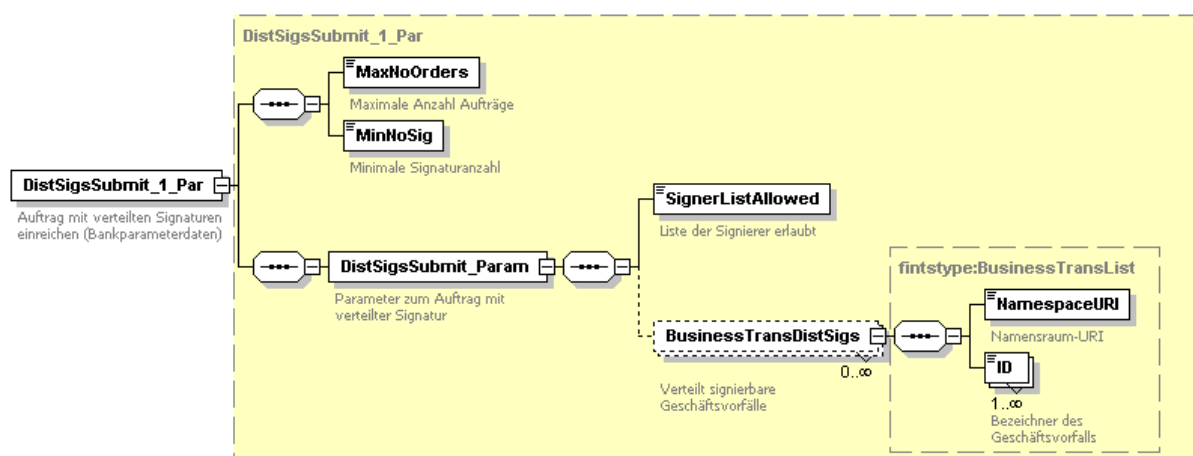


Abbildung 106: Bankparameterdaten Auftrag mit verteilten Signaturen einreichen

III.7.8.2 Informationen zu Auftrag mit verteilten Signaturen

Mit diesem Auftrag kann ein Benutzer sich Informationen zu Aufträgen geben lassen, für die er weitere Signaturen erstellen möchte, insbesondere die zu signierenden Daten selbst (siehe [Formals], Abschnitt III.8 Verteilte Signaturen).

a) Benutzerauftrag

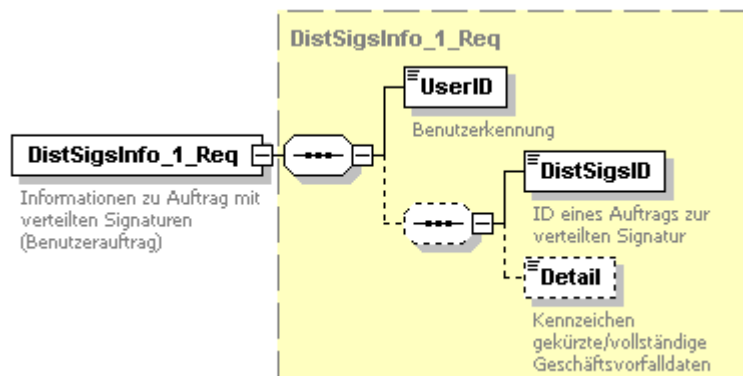


Abbildung 107: Benutzerauftrag Informationen zu Auftrag mit verteilten Signaturen

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 101 |

Detail

Es kann zwischen der gekürzten und der vollen Darstellung des zu signierenden Geschäftsvorfalles gewählt werden. Die zugehörigen Belegungen des Feldes sind *abbreviated* und *complete*.

b) Kreditinstitutsrückmeldung

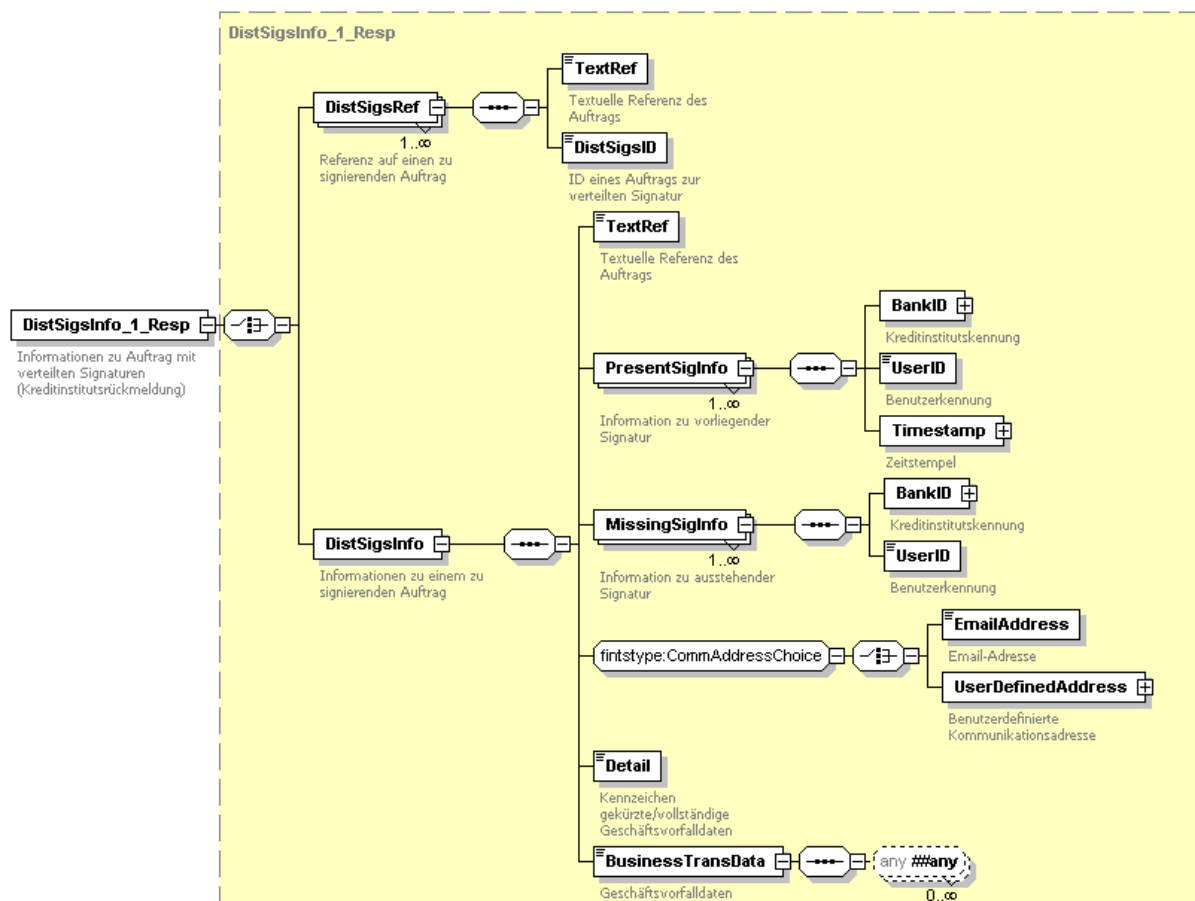


Abbildung 108: Kreditinstitutsrückmeldung Informationen zu Auftrag mit verteilten Signaturen

Geschäftsvorfalldaten

Auftrag oder Auftragsteil, den der Benutzer mit dem Folgeauftrag ‚Auftrag mit verteilter Signatur signieren‘ signieren soll.

c) Bankparameterdaten

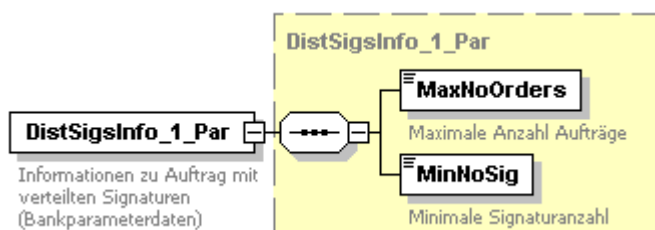


Abbildung 109: Bankparameterdaten Informationen zu Auftrag mit verteilten Signaturen

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 102 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

III.7.8.3 Auftrag mit verteilten Signaturen signieren

Mit diesem Auftrag kann ein Benutzer einen eingereichten Auftrag mit einer weiteren Signatur versehen (siehe [Formals], Abschnitt *III.8 Verteilte Signaturen*).

a) Benutzerauftrag

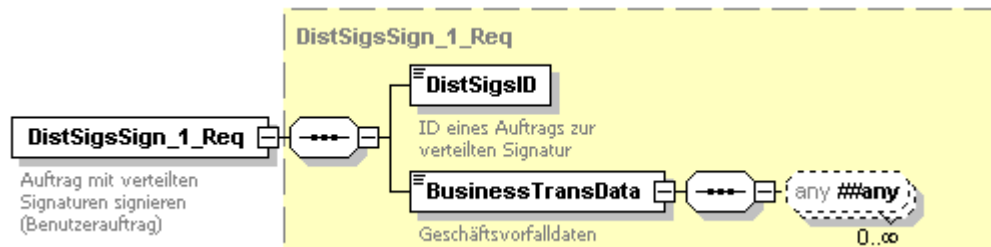


Abbildung 110: Benutzerauftrag Auftrag mit verteilten Signaturen signieren

Auftrag/Auftragsteil

Auftrag oder Auftragsteil, der dem Benutzer bei einer Anforderung zugesandt wurde. Dieser wird vom Benutzer signiert.

b) Kreditinstitutsrückmeldung

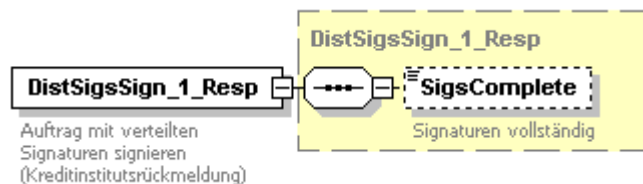


Abbildung 111: Kreditinstitutsrückmeldung Auftrag mit verteilten Signaturen signieren

c) Bankparameterdaten

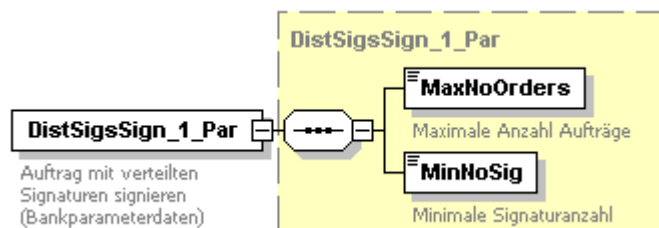


Abbildung 112: Bankparameterdaten Auftrag mit verteilten Signaturen signieren

III.7.8.4 Auftrag mit verteilten Signaturen löschen

Mit diesem Auftrag kann ein Benutzer einen Auftrag löschen, der zur verteilten Signatur eingereicht wurde (siehe [Formals], Abschnitt *III.8 Verteilte Signaturen*).

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 103 |

a) Benutzerauftrag

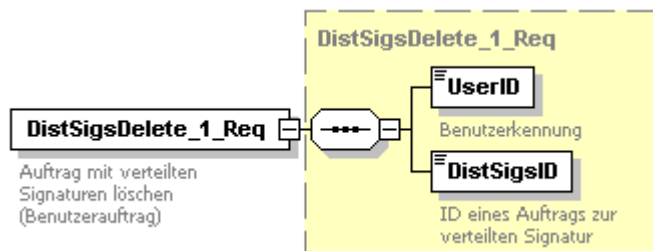


Abbildung 113: Benutzerauftrag Auftrag mit verteilten Signaturen löschen

b) Kreditinstitutsrückmeldung

Die Kreditinstitutsrückmeldung ist leer.

c) Bankparameterdaten

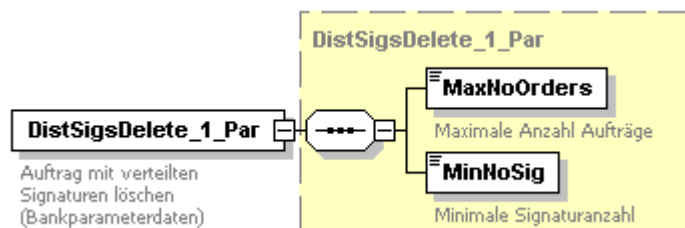


Abbildung 114: Bankparameterdaten Auftrag mit verteilten Signaturen löschen

III.7.9 Statusprotokoll

Im Statusprotokoll verwaltet das Kreditinstitut den Bearbeitungsstatus und die Rückmeldungen der vom Benutzer eingereichten Nachrichten und Aufträge.

III.7.9.1 Statusprotokoll

Mit diesem Auftrag kann ein Benutzer sich das Statusprotokoll anzeigen lassen (siehe [Formals], Abschnitt III.2 Statusprotokoll).

| | | |
|-----------------|----------------------|--|
| Kapitel: III | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 104 | Stand: 09.07.2004 | Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge |

a) Benutzerauftrag

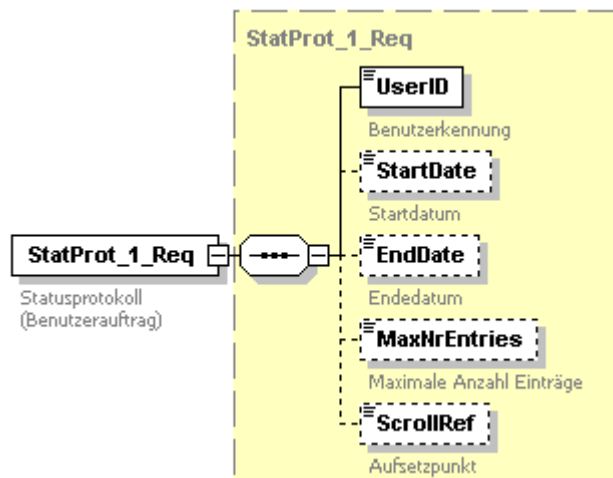


Abbildung 115: Benutzerauftrag Statusprotokoll

b) Kreditinstitutsrückmeldung

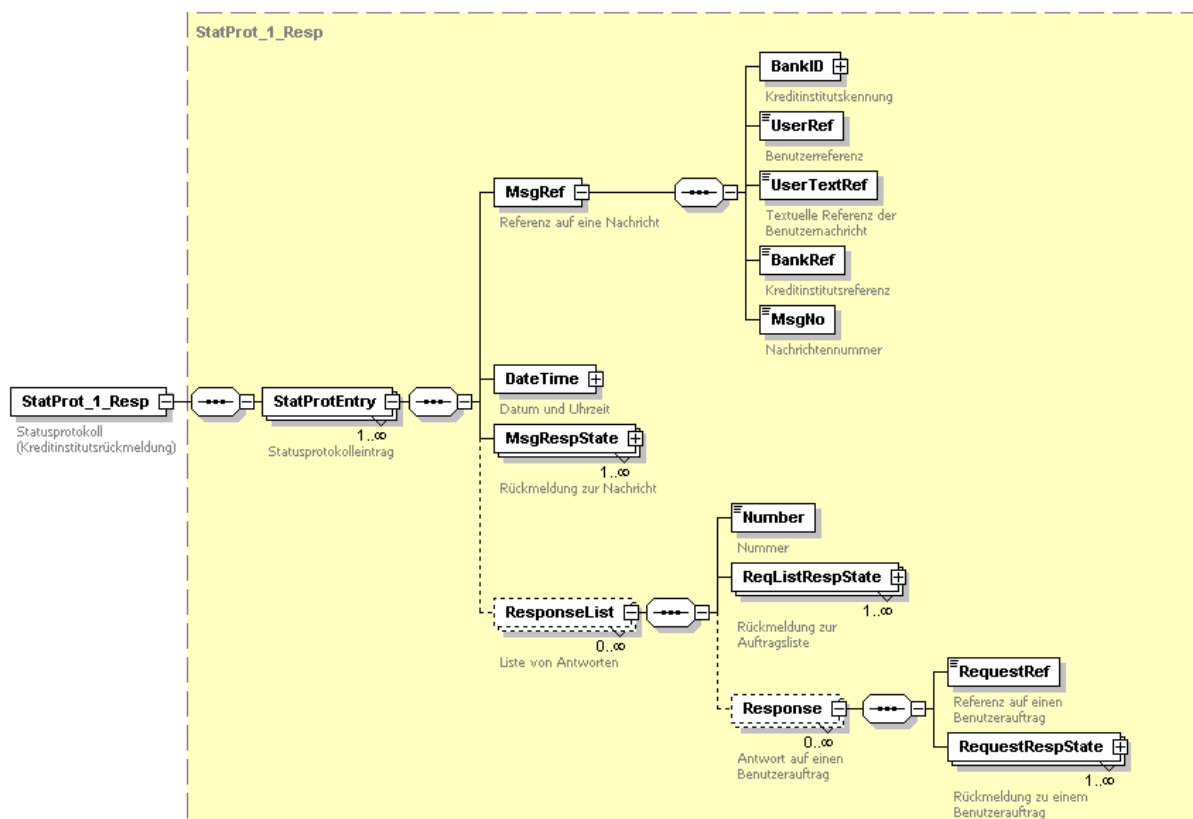


Abbildung 116: Kreditinstitutsrückmeldung Statusprotokoll

Nummer

Das Element bezeichnet die Nummer der Antwortliste der Kreditinstitutsnachricht, beginnend mit Eins.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: III |
| Kapitel: Nachrichtenaufbau Abschnitt: Administrative Aufträge | Stand: 09.07.2004 | Seite: 105 |

c) Bankparameterdaten

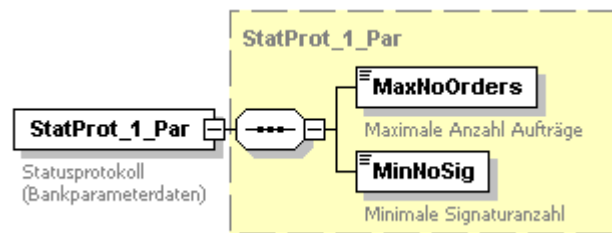


Abbildung 117: Bankparameterdaten Statusprotokoll

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 106 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Administrative Aufträge |

IV. SIGNIERTE NACHRICHTENTEILE

| | |
|--|------------|
| IV.1 Überblick..... | 107 |
| IV.2 Signaturtypen | 108 |
| IV.2.1 [HBCI]-Verfahren: W3C-konforme XML-Signatur | 109 |
| IV.2.2 PIN/TAN-Verfahren | 117 |
| IV.2.3 Benutzerdefinierte Signatur | 118 |
| IV.3 Botensignatur..... | 121 |
| IV.3.1 W3C-konforme XML-Signatur | 122 |
| IV.3.2 PIN/TAN-Verfahren | 124 |
| IV.3.3 Benutzerdefinierte Signatur | 124 |
| IV.4 Auftragssignatur | 125 |
| IV.4.1 W3C-konforme XML-Signatur | 126 |
| IV.4.2 PIN/TAN-Verfahren | 129 |
| IV.4.3 Benutzerdefinierte Signatur | 129 |

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Überblick | Stand: 09.07.2004 | Seite: 107 |

IV.1 Überblick

Die FinTS-Syntax spezifiziert drei unterschiedliche Nachrichtentypen, die für verschiedene Sicherheitsverfahren zum Einsatz kommen. Abschnitt *IV.2 Signaturtypen* beschreibt diese Typen.

In FinTS-Nachrichten können Nachrichten auf zwei Ebenen signiert werden. Die Botensignatur bezieht sich auf alle Aufträge im Nachrichtenkörper. Eine Auftragssignatur hingegen bezieht sich auf Geschäftsvorfälle bzw. administrative Aufträge eines Auftragsteils.

Belegungshinweise und Beispiele für Boten- und Auftragssignaturen finden sich in den Abschnitten *IV.3 Botensignatur* bzw. *IV.4 Auftragssignatur*.

Bei der Angabe von Grammatiken für die Bildung von Lokalisierungspfaden gelten die Festlegungen in *II.8 Referenzierung mit XPath-Ausdrücken*.

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 108 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

IV.2 Signaturtypen

Auf beiden Nachrichtenebenen können drei verschiedene Signaturformen auftreten. Die drei Signaturformen werden für Benutzernachrichten durch die Gruppe *SigChoiceReq* modelliert. Das Inhaltsmodell von *SigChoiceReq* ist so definiert, dass wahlweise [XML Signature]-konform (siehe auch Sicherheitsverfahren [HBCI], Abschnitt *II.5.1 Signatur-Segment*), nach dem PIN/TAN-Verfahren (siehe auch Sicherheitsverfahren [PINTAN], Abschnitt *II.5.1 PIN/TAN-Signatur*) oder nach einem benutzerdefinierten Verfahren signiert werden kann.

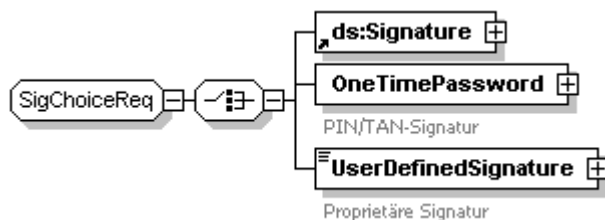


Abbildung 118: Signatur einer Benutzernachricht

Für die Kreditinstitutsnachrichten existieren dieselben Signaturformen. Analog zur Auftragssignatur enthält die Gruppe *SigChoiceResp* eine Auswahlliste mit den drei Signaturformen:

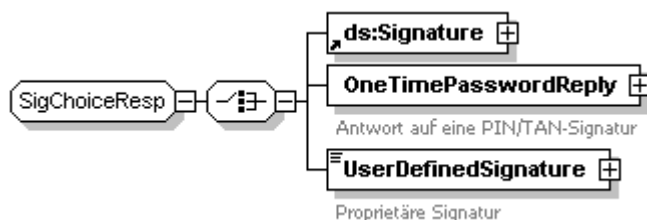


Abbildung 119: Signatur einer Kreditinstitutsnachricht

Die folgenden Abschnitte beschreiben das W3C-konforme Signaturverfahren, das PIN/TAN-Verfahren und die benutzerdefinierte Signatur.

IV.2.1 [HBCI]-Verfahren: W3C-konforme XML-Signatur

Eine XML-Signatur nach Spezifikation des W3C hat den folgenden Aufbau:

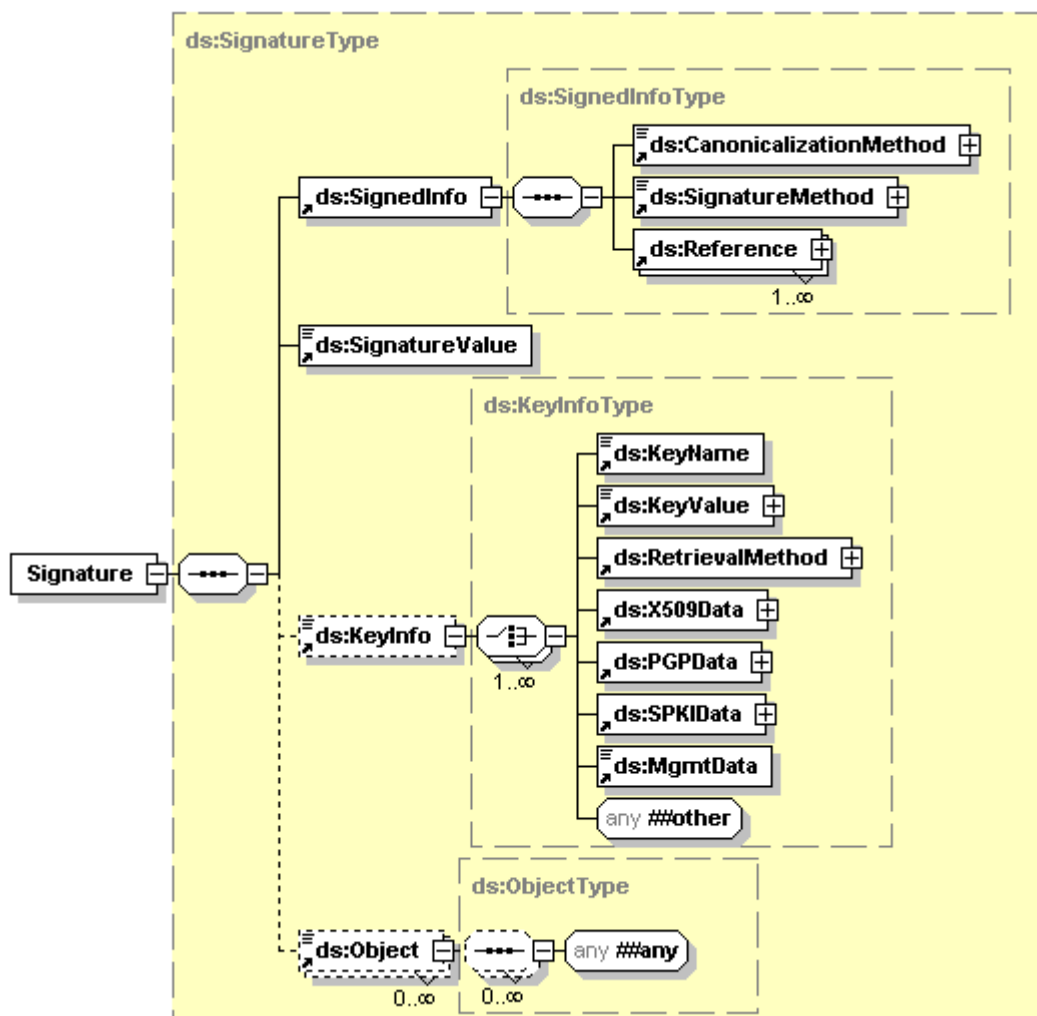


Abbildung 120: Element Signature

Signaturen für Benutzernachrichten und Kreditinstitutsnachrichten sind gleich aufgebaut. Zur Verwendung und Belegung der Signaturen siehe auch [HBCI], Abschnitt II.5.1 Signatur-Segment.

◆ Namespace

Die Elemente dieser Signatur liegen im Namensraum <http://www.w3.org/2000/09/xmldsig#>, der an das Präfix *ds* gebunden wird.

◆ Kanonisierung

Das Element *CanonicalizationMethod* enthält die Angabe des verwendeten Algorithmus zur Kanonisierung des *SignedInfo*-Elements.

Für FinTS-Anwendungen ist in Boten- und Auftragssignaturen das Kanonisierungsverfahren [Exclusive Canonical XML] vorgeschrieben. Erläuterung:

Die Kanonisierung eines XML-Dokuments ist die Überführung eines XML-Fragments bzw. einer Knotenmenge in einheitlicher Form in einen Bytestrom. Diese einheitliche Form ermöglicht die Prüfung einer Signatur. Manipuliert beispielsweise

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 110 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

eine verarbeitende XML-Anwendung ein XML-Dokument durch Einfügen von Leerzeichen in Start- und Endtags oder durch Änderung der Attributreihenfolge, ist die Semantik davon unbeeinträchtigt, die Signaturen jedoch verlieren ihre Gültigkeit. Dieses lässt sich vermeiden, wenn die Signatur auf ein kanonisiertes XML-Fragment gebildet wird.

Das Verfahren [Exclusive Canonical XML] normalisiert ein XML-Fragment ohne den dazugehörigen Kontext.

Beispiel:

Zum Kanonisieren des Elements *SignedInfo* nach dem Verfahren [Exclusive Canonical XML] ist das Attribut *Algorithm* des Elements *CanonicalizationMethod* mit dem Wert <http://www.w3.org/2001/10/xml-exc-c14n#> zu belegen:

```
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
  <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
    PrefixList="ds fintstype fintstrans"/>
</ds:CanonicalizationMethod>
```

Im Attribut *PrefixList* des Elements *InclusiveNamespaces* werden Namensraum-Präfixe aufgelistet, die in den Lokalisierungspfaden der verwendeten XPath-Ausdrücke, ansonsten aber nicht als Element-Präfix innerhalb der Signatur verwendet werden. Mit dieser Auflistung werden sie bei einer Kanonisierung des *SignedInfo* mit in die kanonisierte Darstellung übernommen, so dass die XPath-Ausdrücke gültig bleiben.

♦ Signaturverfahren und Signaturwert

Das Signaturverfahren (*SignatureMethod*) im *SignedInfo*-Element legt den Algorithmus fest, der zur Berechnung des Signaturwerts (*SignatureValue*) verwendet wird.

Die zulässigen Verfahren sind durch die Sicherheitsprofile des Sicherheitsverfahrens [HBCI] festgelegt. Der Signaturwert einer XML-Signatur wird durch Anwendung des Signaturverfahrens auf das kanonisierte *SignedInfo*-Element berechnet und in base64-Codierung in das Element eingestellt.

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen | Stand: 09.07.2004 | Seite: 111 |

◆ Signierte Inhalte

Die durch die XML-Signatur signierten Inhalte werden durch die Referenzen (*Reference*) im *SignedInfo*-Element bestimmt. In FinTS ist genau ein Reference-Element pro Signatur zu verwenden. Die Referenzierung mehrerer Dokumententeile in einer Signatur wird durch den Vereinigungsoperator im XPath-Ausdruck ermöglicht.

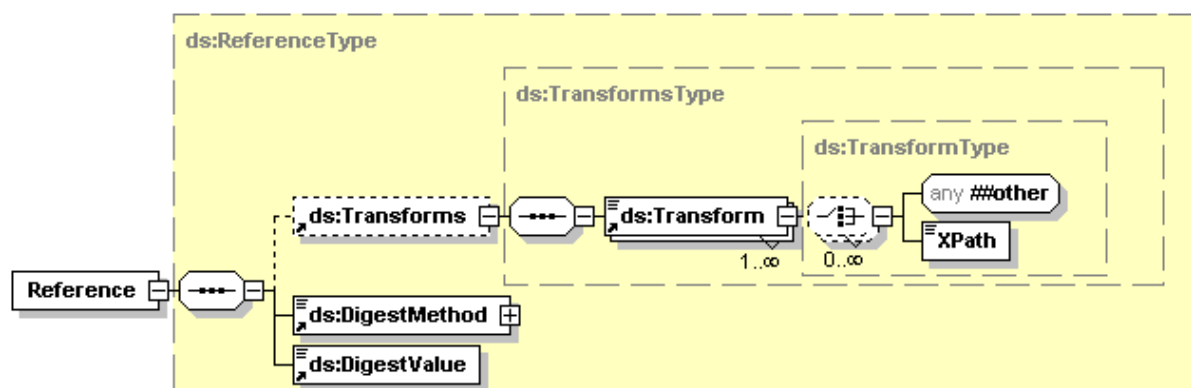


Abbildung 121: Element Reference

Das *Reference*-Element enthält einen Bezeichner (*DigestMethod*) für einen Algorithmus zur Berechnung des Hashwertes, den Hashwert (*DigestValue*), sowie ein *Transforms*-Element, welches die zu signierenden Daten referenziert.

Die zulässigen Hashalgorithmen sind durch die Sicherheitsprofile des Sicherheitsverfahrens festgelegt (siehe [HBCI], Abschnitt *II.1.1 Sicherheitsprofile*). Der Hashwert einer Referenz wird durch Anwendung des Hashalgorithmus auf das Ergebnis der *Transform*-Kette gebildet.

Die Transformation wird durch eine geordnete Abfolge einzelner Transformationsschritte (*Transform*) beschrieben. In FinTS sind genau zwei *Transform*-Elemente verpflichtend:

1. Für den ersten Transformationsschritt ist ausschließlich das Verfahren [XPath Filter], mit genau einem XPath-Ausdruck des Filtertyps *intersect* erlaubt. Der einzustellende Ausdruck für das Element *XPath* ist nach den allgemeinen Regeln für Lokalisierungspfade in *II.8 Referenzierung mit XPath-Ausdrücken* zu bilden.

In den Abschnitten *IV.3 Botensignatur* und *IV.4 Auftragssignatur* wird festgelegt und anhand von Beispielen erläutert, wie diese Regeln für die Verwendung in Boten- und Auftragssignaturen anzuwenden sind.

2. Das Ergebnis des ersten Transformationsschrittes wird im zweiten Schritt in die kanonische Form überführt. Hierzu ist in Boten- und Auftragssignaturen die Verwendung von [Exclusive Canonical XML] Pflicht.

Das *URI*-Attribut des *Reference*-Elements ist in FinTS immer mit der leeren Zeichenkette "" zu belegen

```

<ds:Reference URI="">
  ...
</ds:Reference>

```

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 112 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

◆ Schlüsselinformationen

Das Element *KeyInfo* in Abbildung 121 enthält in Form eines *RDHKeyInfo*- bzw. *DDVKeyInfo*-Elements die Informationen über den Signaturschlüssel gemäß Sicherheitsverfahren [HBCI].

Abbildung 122 zeigt die Schlüsselinformationen für eine XML-Signatur im Sicherheitsverfahren RDH.

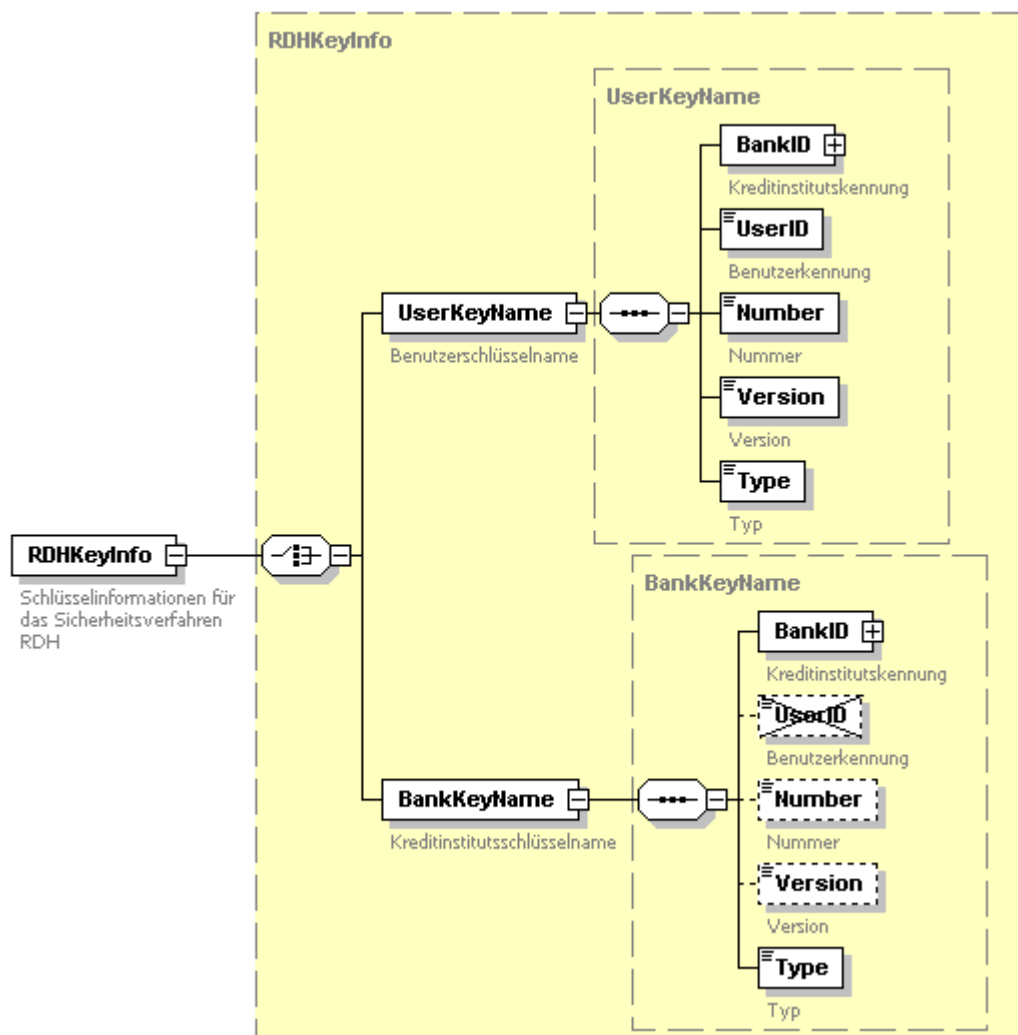


Abbildung 122: Element *RDHKeyInfo*

Benutzerschlüsselname, Kreditinstitutsschlüsselname

In Benutzernachrichten wird der Benutzerschlüsselname belegt, in Kreditinstitutsnachrichten der Kreditinstitutsschlüsselname.

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen | Stand: 09.07.2004 | Seite: 113 |

Abbildung 123 zeigt die Schlüsselinformationen für eine XML-Signatur im Sicherheitsverfahren DDV.

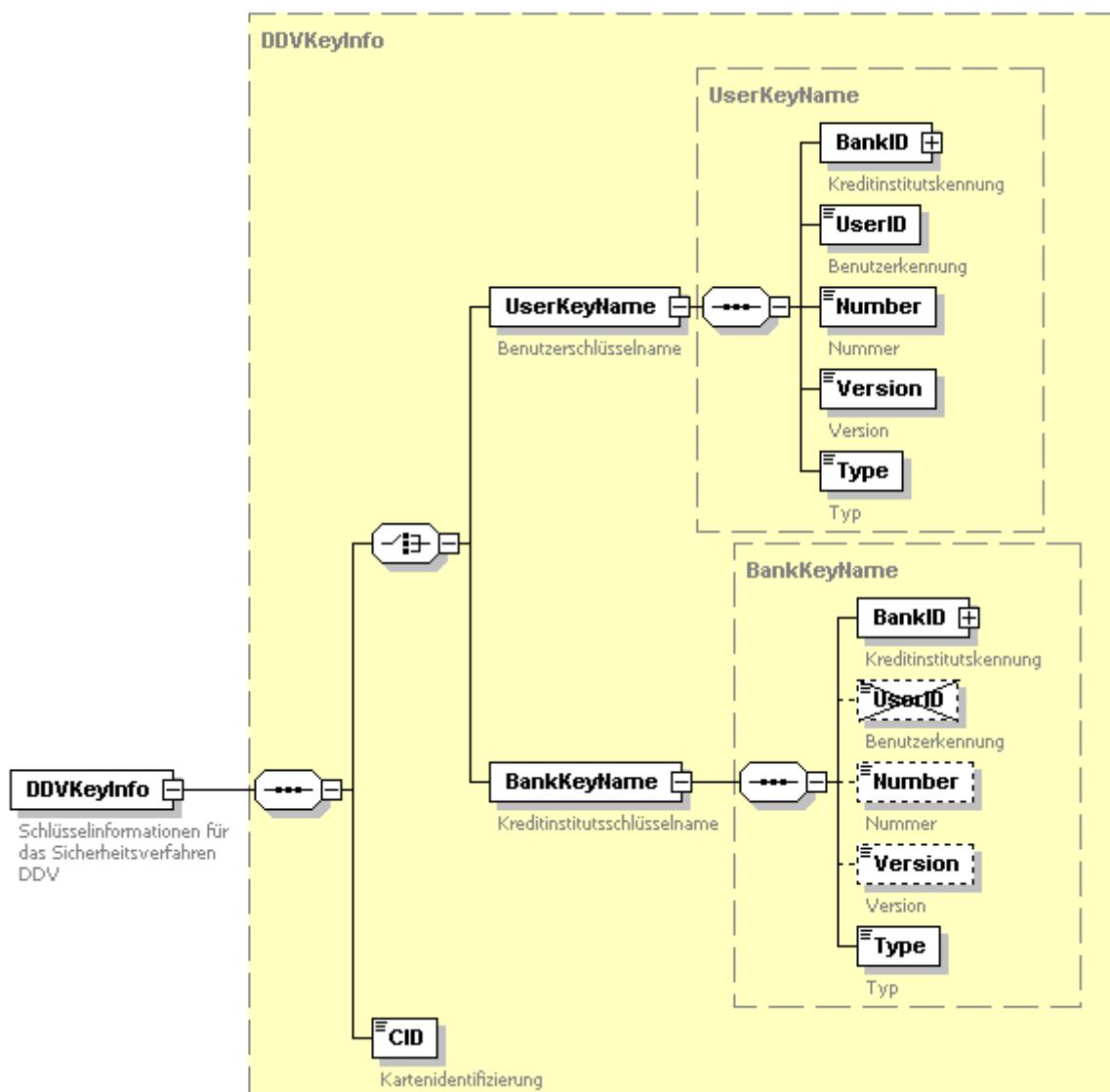


Abbildung 123: Element DDVKeyInfo

Benutzerschlüsselname, Kreditinstitutsschlüsselname

In Benutzernachrichten wird der Benutzerschlüsselname belegt, in Kreditinstitutsnachrichten der Kreditinstitutsschlüsselname.

Kartenidentifizierung

Dieses Feld wird in Kreditinstitutsnachrichten leer gelassen.

Typ

Obwohl im DDV-Verfahren keine unterschiedlichen Schlüssel existieren, wird dieses Element wie im RDH-Verfahren mit dem logischen Typ des für die jeweilige Operation notwendigen Schlüssels belegt.

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 114 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

♦ Signatureigenschaften

Unter dem Element *Object* können beliebige Zusatzinformationen zur Signatur als *SignatureProperties* transportiert werden. In FinTS werden dort innerhalb eines *SignatureProperty*-Elements die FinTS-spezifischen Signatureigenschaften in Form eines *DDVProperty*- bzw. *RDHProperty*-Elements hinterlegt.

Beispiel:

```
<ds:Signature Id="28099950001Ben-000000012-1228743211628"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  ...
  <ds:Object>
    <ds:SignatureProperties>
      <ds:SignatureProperty Target="#28099950001Ben-000000012-1228743211628">
        <fintstype:RDHProperty>
          ...
        </fintstype:RDHProperty>
      </ds:SignatureProperty>
    </ds:SignatureProperties>
  </ds:Object>
</ds:Signature>
```

Das Pflichtattribut *Target* verweist auf die Signatur zu der die Signatureigenschaften gehören, in FinTS somit auf das *Signature*-Element, in das die Properties eingebettet sind.



Verweisziel des *Target*-Attributs ist das *Id*-Attribut der Signatur. Diese *Id* muss im gesamten Dokument eindeutig sein.



Damit auch im Intermediärszenario keine Kollisionen zwischen den - von verschiedenen Benutzern erstellten - Ids auftreten, wird für Kundensysteme folgende Belegungsrichtlinie empfohlen: die Id wird gebildet durch Konkatenation von Länderkennzeichen, Kreditinstitutscode, Benutzerkennung, Kundensystemkennung und Signatur-ID.

Das Kreditinstitut muss in seinen Nachrichten ebenfalls auf Eindeutigkeit der Ids innerhalb einer Nachricht achten.

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen | Stand: 09.07.2004 | Seite: 115 |

Abbildung 124 zeigt die spezifischen Parameter für eine XML-Signatur im Sicherheitsverfahren RDH.

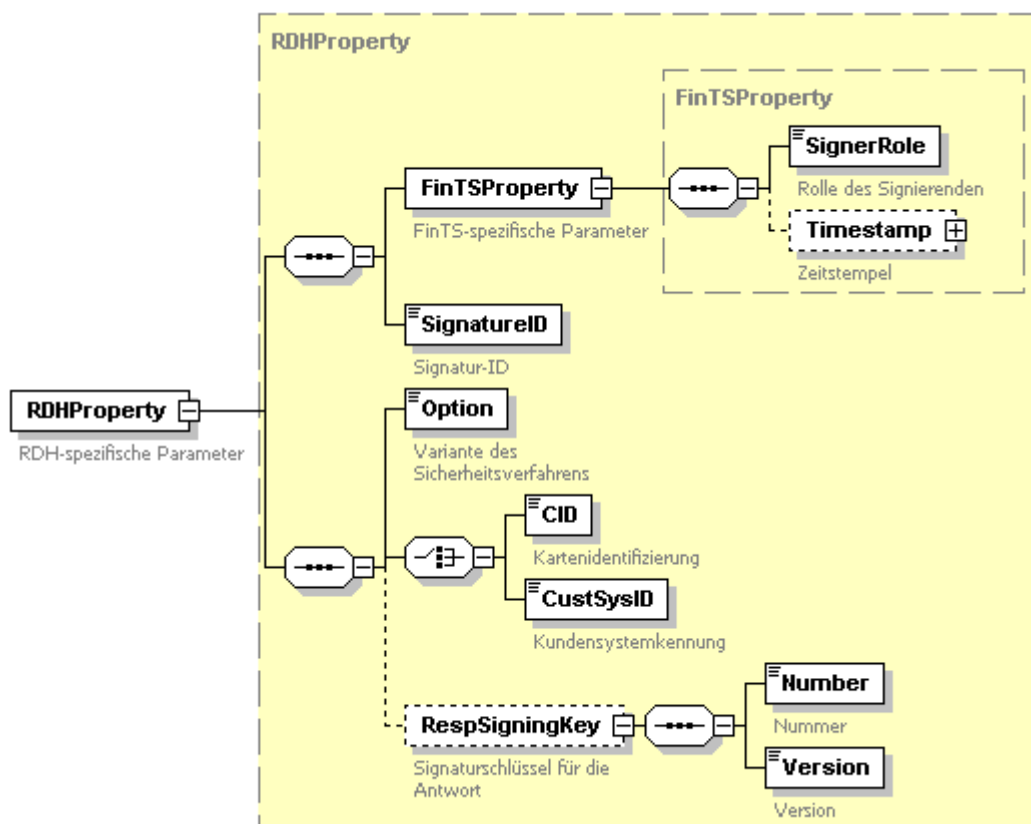


Abbildung 124: Element RDHProperty

Signatur Schlüssel für die Antwort

In der Benutzernachricht ist dieses Element Pflicht, sofern das Kreditinstitut seine Nachrichten signiert. In der Kreditinstitutsnachricht entfällt es.

Variante des Sicherheitsverfahrens

In diesem Element stellt der Signierende die Variante des aktuell von ihm verwendeten RDH-Verfahrens (siehe [HBCI], Abschnitt II.1.1 *Sicherheitsprofile*) ein. Ein Benutzer oder Kreditinstitut hat alle Signaturen oder Verschlüsselungen in einem Dokument im selben Sicherheitsprofil vorzunehmen.

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 116 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

Abbildung 125 zeigt die spezifischen Parameter für eine XML-Signatur im Sicherheitsverfahren DDV.

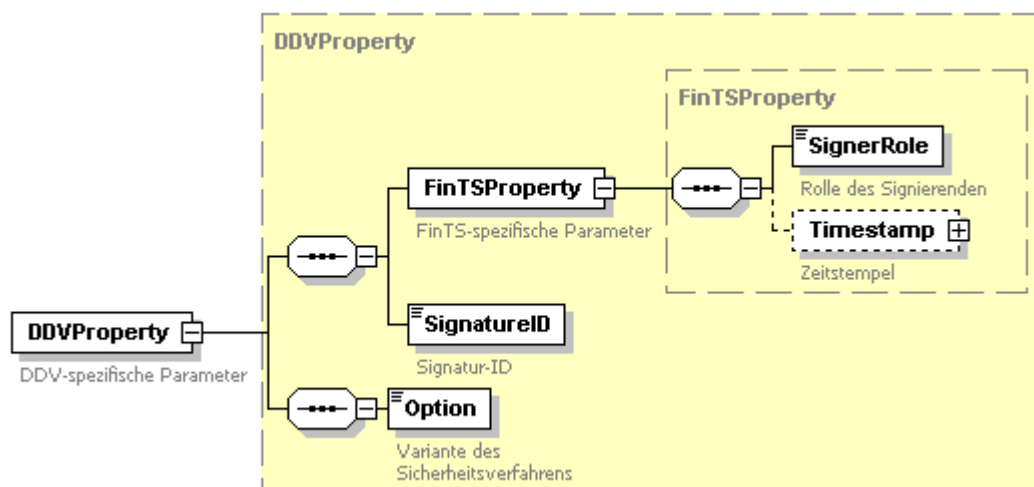


Abbildung 125: Element DDVProperty

Variante des Sicherheitsverfahrens

In diesem Element stellt der Signierende die Variante des aktuell von ihm verwendeten DDV-Verfahrens (siehe [HBCI], Abschnitt II.1.1 *Sicherheitsprofile*) ein. Ein Benutzer oder Kreditinstitut hat alle Signaturen oder Verschlüsselungen in einem Dokument im selben Sicherheitsprofil vorzunehmen.

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen | Stand: 09.07.2004 | Seite: 117 |

IV.2.2 PIN/TAN-Verfahren

Für die Signatur einer Benutzernachricht im Verfahren PIN/TAN wird das Element *OneTimePassword* verwendet. Zur Verwendung und Belegung der Signatur siehe auch [PINTAN], Abschnitt II.5.1 *PIN/TAN-Signatur*.

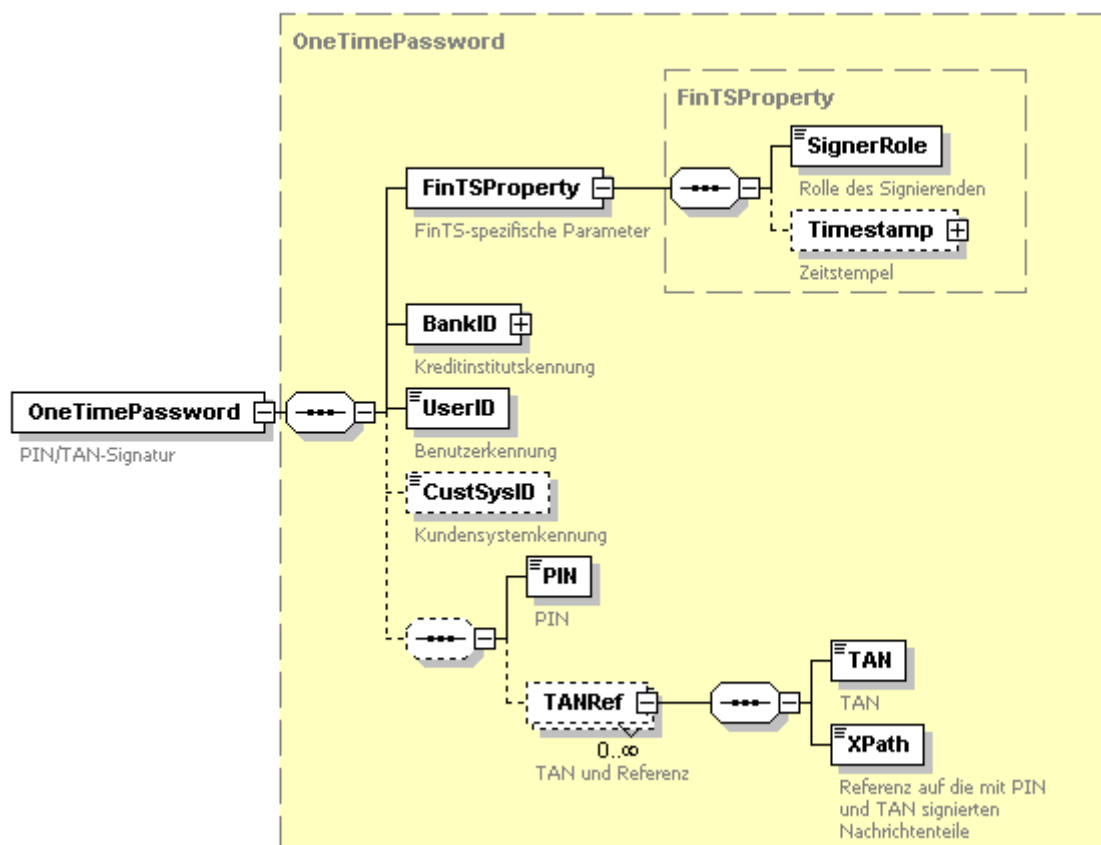


Abbildung 126: Element *OneTimePassword*

Referenz auf die mit PIN und TAN signierten Nachrichtenteile

In den Abschnitten IV.3 *Botensignatur* und IV.4 *Auftragssignatur* wird festgelegt und anhand von Beispielen gezeigt, wie die XPath-Referenzen in Boten- und Auftragssignaturen zu verwenden sind.

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 118 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

Die Signatur der Kreditinstitutsnachricht wird im Element *OneTimePasswordReply* übertragen. Es gelten die Festlegungen aus [PINTAN], Abschnitt II.5.2 *Antwort auf eine PIN/TAN-Signatur*.

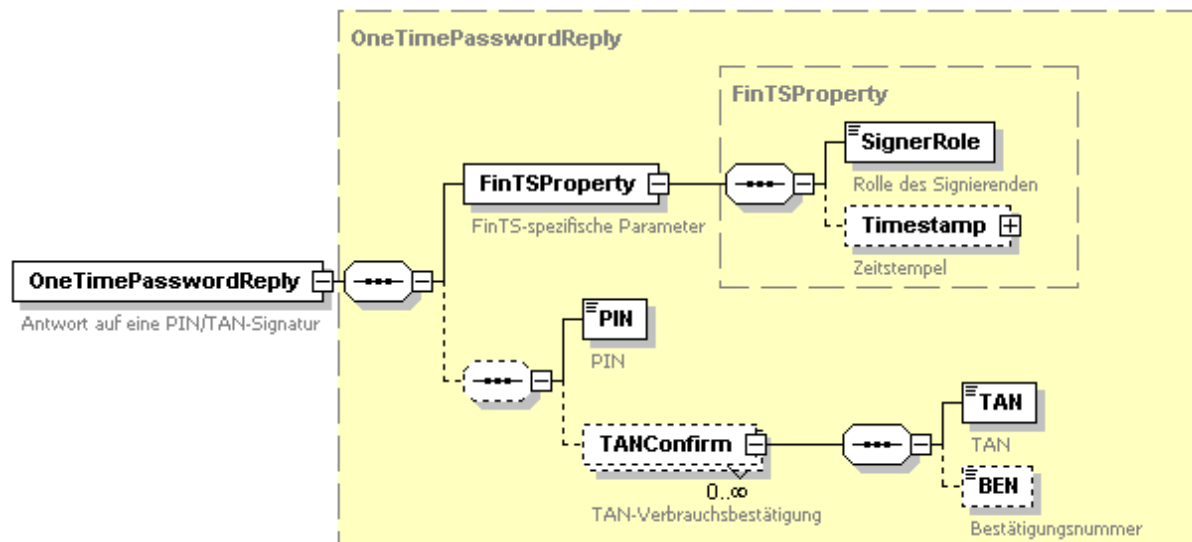


Abbildung 127: Element *OneTimePasswordReply*

IV.2.3 Benutzerdefinierte Signatur

Eine benutzerdefinierte Signatur besteht aus einem festen Rahmen *UserDefinedSignature*, welcher ein beliebiges (benutzerdefiniertes) Inhaltsmodell aufweist. Mit „benutzerdefiniert“ ist hier eine bilaterale Vereinbarung zwischen einem Kreditinstitut und Benutzern oder Benutzergruppen gemeint bzw. die Definition und Veröffentlichung eines Verfahrens durch ein Kreditinstitut oder einen Verband.

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen | Stand: 09.07.2004 | Seite: 119 |

Zur Validierung der XML-Struktur der benutzerdefinierten Signatur kann analog zur Einbettung von Fremdformaten in eine FinTS-Nachricht (siehe *II.6.2 Integration fremder Transaktionsformate in FinTS*) ein XML-Schema angegeben werden.

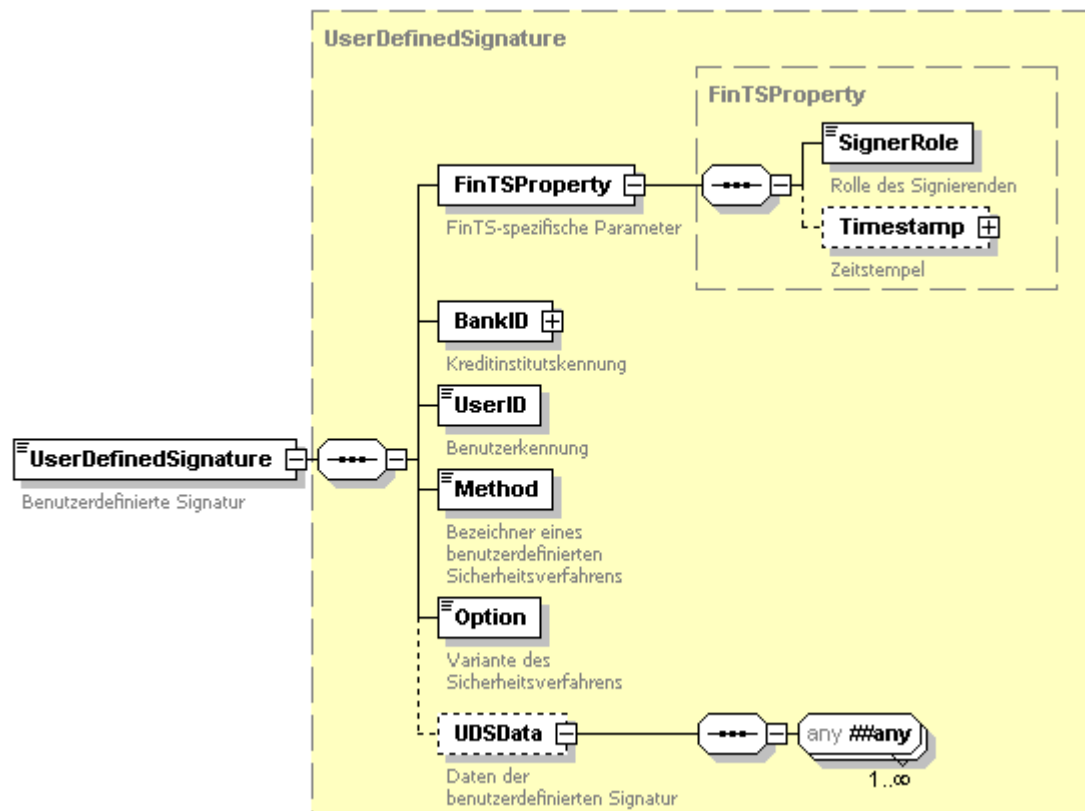


Abbildung 128: Element UserDefinedSignature

Zum festen Rahmen gehören [BankID](#) und [UserID](#), die den signierenden Benutzer [identifizieren](#), sowie ein [FinTSPProperty](#)-Element mit der Rolle des Signierenden ([SignerRole](#)) sowie dem Signaturzeitpunkt ([Timestamp](#)). Weiterhin kann das verwendete Verfahren anhand der Elemente [Method](#) und [Option](#) identifiziert werden, ohne Kenntnis des benutzerdefinierten Inhaltsmodells besitzen zu müssen. Im [Element UDSData](#) können beliebige, bilateral vereinbarte Daten übertragen werden.

Bei diesem Signaturverfahren wird sowohl für Signaturen der Benutzernachricht als auch für Signaturen der Kreditinstitutsnachricht das Element [UserDefinedSignature](#) verwendet.

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 120 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Signaturtypen |

Beispiel:

```

<ReqMsg
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.fints.org/spec/xmlschema/4.0/
    http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd">
  ...
  <UserDefinedSignature>
    <FinTSProperty>
      <SignerRole>ISS</SignerRole>
      <Timestamp>
        <Date>2003-10-03</Date>
        <Time>14:59:13</Time>
      </Timestamp>
    </FinTSProperty>
    <BankID>
      <CountryCode>280</CountryCode>
      <BankCode>99950001</BankCode>
    </BankID>
    <UserID>mySigUser</UserID>
    <Method>MySignature#Identifier</Method>
    <Option>Type0</Option>
    <UDSData>
      <MySignature>
        xmlns="mySig-Namensraum-URI"
        xsi:schemaLocation="mySig-Namensraum-URI mySig.xsd"
        ...
      </MySignature>
    </UDSData>
  </UserDefinedSignature>
  ...
</ReqMsg>

```

Bei benutzerdefinierten Signaturen wird die Festlegung eines Schemas sowie eines Namensraumes für das Schema empfohlen. Im Beispiel wird bei der benutzerdefinierten Signatur das Schema *mySig.xsd* zur Validierung angegeben.

| | | |
|---|-------------------|-------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Botensignatur | Stand: 09.07.2004 | Seite: 121 |

IV.3 Botensignatur

Ein Kreditinstitut kann alle acht Nachrichtentypen mit einer Botensignatur versehen. Ein Benutzer signiert dagegen lediglich die Nachrichtentypen *StandardReq*, *SynchronisationReq*, *UserKeyTransmissionReq*, *KeyChangeReq* und *KeyBlockReq*.

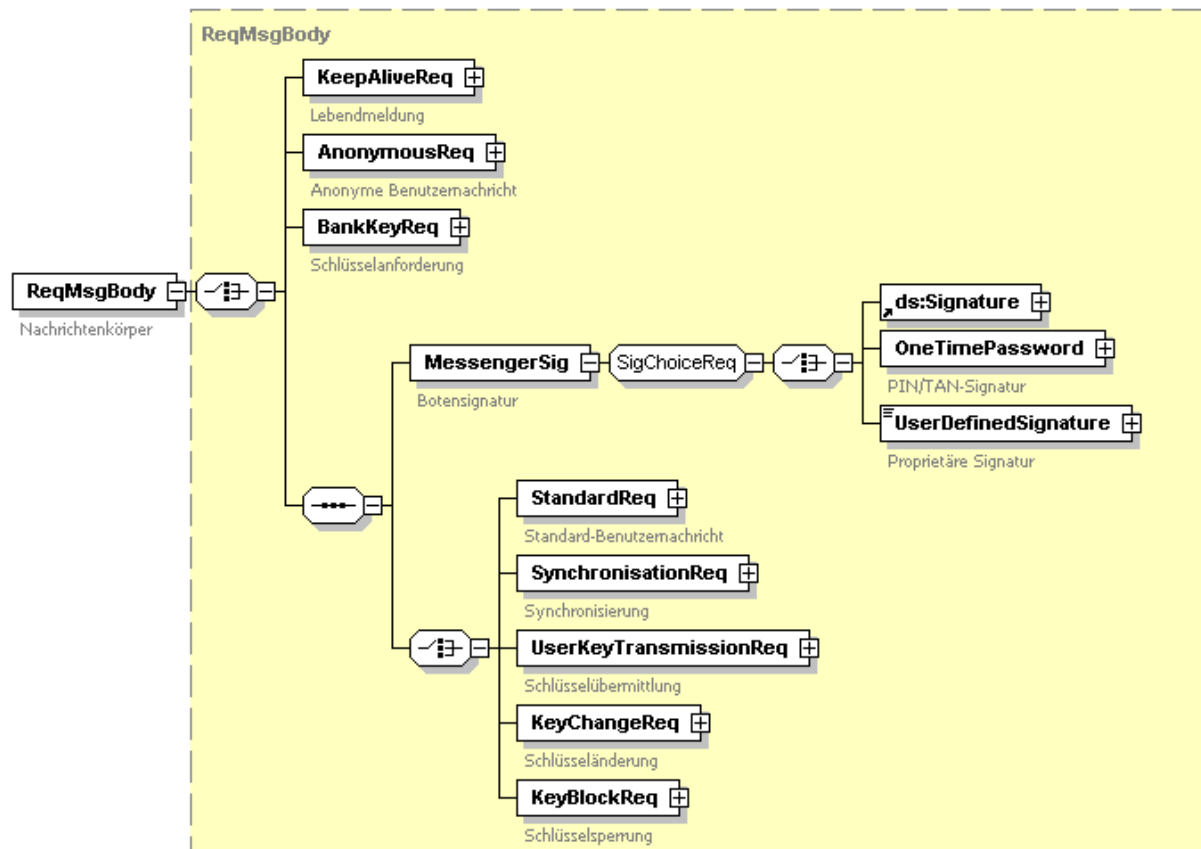


Abbildung 129: Botensignatur im Nachrichtenkörper einer Benutzernachricht

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 122 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Botensignatur |

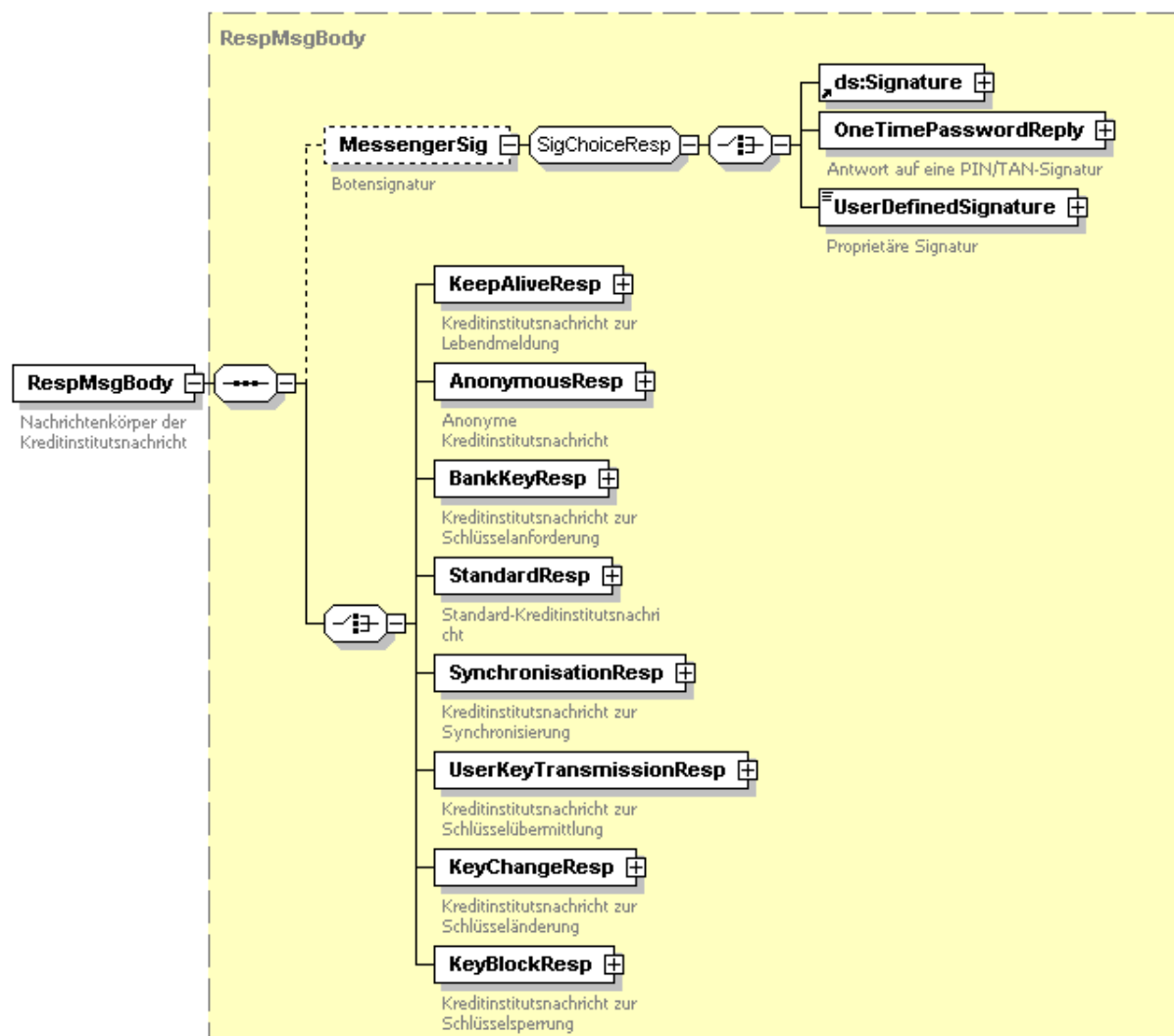


Abbildung 130: Botensignatur im Nachrichtenkörper der Kreditinstitutsnachricht

IV.3.1 W3C-konforme XML-Signatur

Die Referenzen werden bei einer Botensignatur wie folgt verwendet:

| | |
|---------------------|---|
| Referenz-Ziele | <p>Die folgenden Ziele sind verpflichtend anzugeben:</p> <ul style="list-style-type: none"> Nachrichtenkopf (<i>ReqMsgHeader</i> in Benutzernachrichten oder <i>RespMsgHeader</i> in Kreditinstitutsnachrichten) Inhalt des Nachrichtenkörpers (je nach Nachrichtentyp: <i>StandardReq</i>, <i>StandardResp</i>, <i>SyncReq</i> etc.) eigenes <i>ds:Object</i>-Element |
| Gültigkeitsbereich | <p>Wurzelement der Nachricht</p> <ul style="list-style-type: none"> <i>ReqMsg</i> in Benutzernachrichten oder <i>RespMsg</i> in Kreditinstitutsnachrichten |
| Zulässiger Ausdruck | <p>Der XPath-Ausdruck für die [XPath Filter]-Transformation muss der Bildungsregel für <i>LocationPath</i> genügen:</p> <pre> LocationPath ::= SinglePath (' ' SinglePath)* SinglePath ::= AbsoluteLocationPath ::= HereLocationPath </pre> |

| | | |
|---|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Botensignatur | Stand: 09.07.2004 | Seite: 123 |

Das folgende Beispiel zeigt eine W3C-konforme XML-Signatur als Botensignatur und die Syntax der XPath-Referenzen für eine FinTS- Benutzernachricht:

```
<MessengerSig xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <ds:Signature Id="28099950001Ben-900312-1228743211052905678156"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
          PrefixList="ds fintstype fintstrans"/>
        </ds:CanonicalizationMethod>
      <ds:SignatureMethod
        Algorithm="http://www.fints.org/spec/xmlschema/4.0/final/xmldsig#rsa-
        ripemd160-iso9796-1"/>
      <ds:Reference URI="">
        <ds:Transforms>
          <ds:Transform
            Algorithm=" http://www.w3.org/2002/06/xmldsig-filter2"
            xmlns:xpf="http://www.w3.org/2002/06/xmldsig-filter2"
            xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types">
              <xpf:XPath
                Filter="intersect"/>/fintstype:ReqMsg[1]/fintstype:ReqMsgHeader[1]
                |fintstype:ReqMsg[1]/fintstype:ReqMsgBody[1]/fintstype:StandardReq[1]
                |fintstype:ReqMsg[1]/fintstype:ReqMsgBody[1]/fintstype:MessengerSig[1]/ds:Object[1]</
                xpf:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
                <ec:InclusiveNamespaces
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                  PrefixList="ds fintstype fintstrans"/>
                </ds:Transform>
              </ds:Transforms>
            <ds:DigestMethod
              Algorithm="http://www.w3.org/2001/04/xmldsig#ripemd160"/>
            <ds:DigestValue> DEADBEEF...KIrUsd</ds:DigestValue>
          </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>DEADBEEF...oGrUieN</ds:SignatureValue>
        <ds:KeyInfo>
          <RDHKeyInfo>
            <UserKeyName>
              <BankID>
                <CountryCode>280</CountryCode>
                <BankCode>99950001</BankCode>
              </BankID>
              <UserID>UID926518</UserID>
              <Number>1</Number>
              <Version>1</Version>
              <Type>S</Type>
            </UserKeyName>
          </RDHKeyInfo>
        </ds:KeyInfo>
        <ds:Object>
          <ds:SignatureProperties>
            <ds:SignatureProperty Target="#28099950001Ben-900312-1228743211052905678156">
              <RDHProperty>
                <FinTSProperty>
                  <SignerRole>MSG</SignerRole>
                  <Timestamp>
                    <Date>2003-10-03</Date>
                    <Time>14:59:13</Time>
                  </Timestamp>
                </FinTSProperty>
                <SignatureID>1052905678156</SignatureID>
                <Option>1</Option>
                <CustSysID>KSIdent</CustSysID>
              </RDHProperty>
            </ds:SignatureProperty>
          </ds:SignatureProperties>
        </ds:Object>
      </ds:Signature>
    </MessengerSig>
```

Das Beispiel zeigt die Referenzierung in einer Botensignatur anhand des in ihr enthaltenen *Reference*-Elements. Darin werden die drei referenzierten Nachrichtenteile durch die Vereinigungsoperation | zusammengefasst. Der erste

| | | |
|----------------|----------------------|---|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 124 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Botensignatur |

XPath-Ausdruck referenziert das Element *ReqMsgHeader* der Benutzernachricht, in der die Botensignatur enthalten ist. Die resultierende Knotenmenge wird durch die beiden folgenden Lokalisierungspfade mit den Mengen der Knoten unter *StandardReq* und *ds:Object* vereinigt.

IV.3.2 PIN/TAN-Verfahren

In der Botensignatur einer Benutzernachricht kann optional eine TAN zusammen mit einer Referenz angegeben werden. Wird dieses Element *TANRef* angegeben, gelten die folgenden Festlegungen für das Element *XPath*:

| | |
|---------------------|--|
| Referenz-Ziel | Wurzelement des Nachrichtenkörpers (<i>ReqMsgBody</i>) |
| Gültigkeitsbereich | Wurzelement der Benutzernachricht (<i>ReqMsg</i>) |
| Kontext | Der Kontext zur Auswertung des Lokalisierungspfades ist das Element <i>XPath</i> , in dem sich der Ausdruck befindet. |
| Zulässiger Ausdruck | Der Ausdruck im Element <i>XPath</i> muss der Bildungsregel für <i>LocationPath</i> genügen: $\text{LocationPath} ::= \text{AbsoluteLocationPath} \\ ::= \text{RelativeLocationPath}$ |

Das folgende Beispiel zeigt eine Botensignatur nach dem PIN/TAN-Verfahren in einer Benutzernachricht:

```
<MessengerSig xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <OneTimePassword>
    <FinTSPROPERTY>
      <SignerRole>MSG</SignerRole>
      <Timestamp>
        <Date>2003-10-03</Date>
        <Time>14:59:13</Time>
      </Timestamp>
    </FinTSPROPERTY>
    <BankID>
      <CountryCode>280</CountryCode>
      <BankCode>99950001</BankCode>
    </BankID>
    <UserID>UID926518</UserID>
    <CustSysID>KSIIdent</CustSysID>
    <PIN>123456</PIN>
  </OneTimePassword>
</MessengerSig>
```

Es wird hier implizit die gesamte Nachricht signiert, die Angabe einer TAN sowie eines Referenz-Ziels entfällt.

IV.3.3 Benutzerdefinierte Signatur

Eine benutzerdefinierte Signatur enthält keine im Rahmen des FinTS-Standards spezifizierten Referenzierungen. Die Belegung ist somit identisch bei der Verwendung als Boten- oder Auftragssignatur.

Eine benutzerdefinierte Botensignatur signiert implizit den Nachrichtenkopf und den Inhalt des Nachrichtenkörpers.

IV.4 Auftragssignatur

Mit einer Auftragssignatur werden einzelne Geschäftsvorfälle in einer *RequestList* oder Antworten zu Geschäftsvorfällen in einer *ResponseList* signiert. Eine *RequestList* oder *ResponseList* kann mehrere Auftragssignaturen enthalten, jede Signatur kann einen oder mehrere Geschäftsvorfälle signieren. Die beiden folgenden Abbildungen zeigen die Positionen der Auftragssignaturen in einer Standard-Benutzernachricht und der Standard-Kreditinstitutsnachricht:

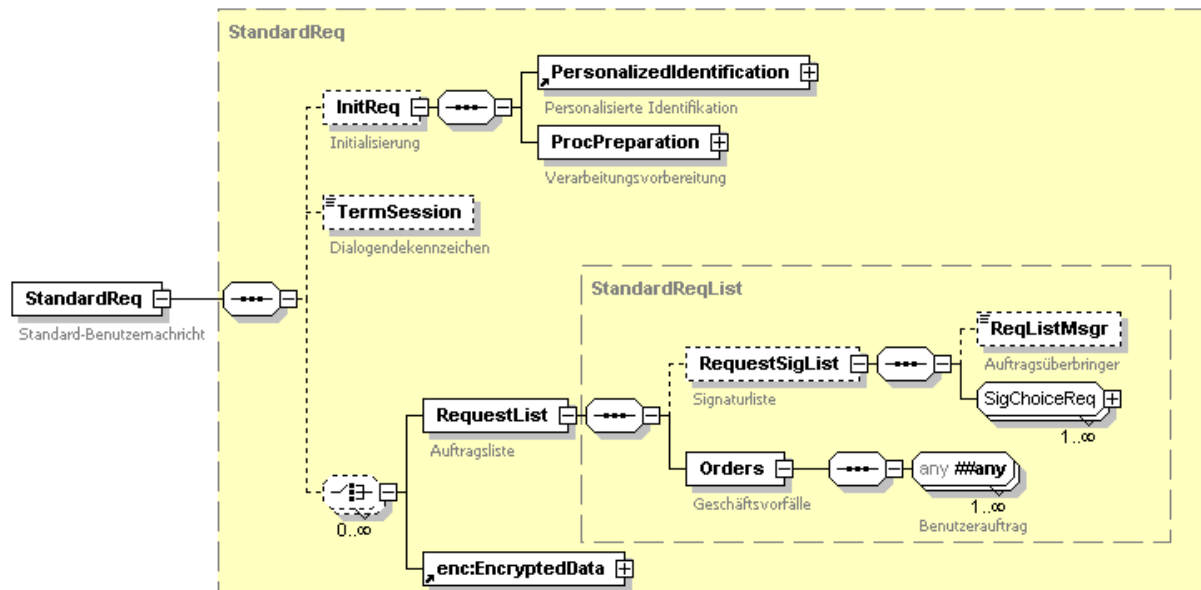


Abbildung 131: Auftragssignatur in einer Benutzernachricht

Auftragsüberbringer

Im Element *ReqListMsgr* wird eine der Signaturen als diejenige des Benutzers gekennzeichnet, für den in der Kreditinstitutsnachricht die entsprechende Liste der Antworten signiert und ggf. verschlüsselt werden soll. Für den hier einzustellenden XPath gelten folgende Regeln:

| | |
|---------------------|--|
| Referenz-Ziele | Genau einer der Geschwisterknoten <ul style="list-style-type: none"> • Signature, • OneTimePassword oder • UserDefinedSignature des Elements <i>ReqListMsgr</i> . |
| Gültigkeitsbereich | Das Elternelement <i>RequestSigList</i> von <i>ReqListMsgr</i> . |
| Kontext | Der Kontext zur Auswertung des Lokalisierungspfades ist das Element <i>ReqListMsgr</i> , in dem sich der Ausdruck befindet. |
| Zulässiger Ausdruck | Der Ausdruck in <i>ReqListMsgr</i> muss der Bildungsregel für <i>RelativeLocationPath</i> genügen. |

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Auftragssignatur | Stand: 09.07.2004 | Seite: 127 |

Das folgende Beispiel zeigt die Signatur eines Geschäftsvorfalles (*AcctBal*):

| | | |
|----------------|----------------------|--|
| Kapitel: IV | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 128 | Stand: 09.07.2004 | Kapitel: Signierte Nachrichtenteile Abschnitt: Auftragssignatur |

```

<RequestList xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <RequestSigList>
    <ReqListMsggr>../ds:Signature[1]</ReqListMsggr>
    <ds:Signature Id="28099950001Ben-900312-1228743211052705938186"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo
        xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types"
        xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions">
          <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces
              xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
              PrefixList="ds fintstype fintstrans"/>
            </ds:CanonicalizationMethod>
          <ds:SignatureMethod
            Algorithm="http://www.fints.org/spec/xmlschema/4.0/final/xmldsig#rsa-
            ripemd160-iso9796-1"/>
          <ds:Reference URI="">
            <ds:Transforms>
              <ds:Transform
                Algorithm="http://www.w3.org/2002/06/xmldsig-filter2"
                xmlns:xpf="http://www.w3.org/2002/06/xmldsig-filter2">
                <xpf:XPath Filter="intersect">here()../../../../../ds:Object[1]
                | here()../../../../../fintstype:Orders[1]/fintstrans:AcctBal_1_Req[1]
                </xpf:XPath>
              </ds:Transform>
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                <ec:InclusiveNamespaces
                  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                  PrefixList="ds fintstype fintstrans"/>
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#ripemd160"/>
              <ds:DigestValue> DEADBEEF...uFeKhU </ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue> DEADBEEF...oFWuWRT</ds:SignatureValue>
          <ds:KeyInfo>
            <RDHKeyInfo>
              <UserKeyName>
                <BankID>
                  <CountryCode>280</CountryCode>
                  <BankCode>99950001</BankCode>
                </BankID>
                <UserID>UID926518</UserID>
                <Number>1</Number>
                <Version>1</Version>
                <Type>S</Type>
              </UserKeyName>
            </RDHKeyInfo>
          </ds:KeyInfo>
          <ds:Object>
            <ds:SignatureProperties>
              <ds:SignatureProperty Target="#28099950001Ben-900312-
              1228743211052705938186">
                <RDHProperty>
                  <FinTSProperty>
                    <SignerRole>ISS</SignerRole>
                    <Timestamp>
                      <Date>2003-10-05</Date>
                      <Time>15:13:45</Time>
                    </Timestamp>
                  </FinTSProperty>
                  <SignatureID>1052705938186</SignatureID>
                  <Option>1</Option>
                  <CustSysID>KSIdent</CustSysID>
                </RDHProperty>
              </ds:SignatureProperty>
            </ds:SignatureProperties>
          </ds:Object>
        </ds:Signature>
      </RequestSigList>
      <Orders>
        <fintstrans:AcctBal_1_Req
          xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
          ...
        </fintstrans:AcctBal_1_Req>
      </Orders>
    </RequestList>
  
```

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: IV |
| Kapitel: Signierte Nachrichtenteile Abschnitt: Auftragssignatur | Stand: 09.07.2004 | Seite: 129 |

IV.4.2 PIN/TAN-Verfahren

In der Auftragssignatur einer Benutzernachricht werden diejenigen Aufträge referenziert, welche mit einer *TAN* signiert werden. Für die Referenzen gelten die folgenden Festlegungen:

| | |
|---------------------|--|
| Referenz-Ziele | In einer Benutzernachricht verweist jeder <i>XPath</i> auf einen beliebigen Benutzerauftrag, also auf ein beliebiges Kindelement des Elements <i>Orders</i> oder der entsprechenden Elemente der administrativen Nachrichten unterhalb der <i>RequestList</i> , in der sich die Signatur befindet. |
| Gültigkeitsbereich | Wurzelement der Liste von Aufträgen (<i>RequestList</i>) in der sich die Signatur befindet: |
| Kontext | Der Kontext zur Auswertung des Lokalisierungspfades ist das Element <i>XPath</i> in dem sich der Ausdruck befindet. |
| Zulässiger Ausdruck | Der Ausdruck in <i>XPath</i> muss der Bildungsregel für <i>RelativeLocationPath</i> genügen. |

Das Beispiel zeigt die Signatur eines Geschäftsvorfalles (*AcctBal*):

```
<RequestList xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <RequestSigList>
    <ReqListMsgr>../fintstype:OneTimePassword[1]</ReqListMsgr>
    <OneTimePassword>
      <FinTSProperty>
        <SignerRole>ISS</SignerRole>
        <Timestamp>
          <Date>2003-10-05</Date>
          <Time>15:13:45</Time>
        </Timestamp>
      </FinTSProperty>
      <BankID>
        <CountryCode>280</CountryCode>
        <BankCode>99950001</BankCode>
      </BankID>
      <UserID>UID926518</UserID>
      <CustSysID>KSIdent</CustSysID>
      <PIN>123456</PIN>
      <TANRef>
        <TAN>123456</TAN>
        <XPath>../../../../fintstype:Orders[1]/fintstrans:AcctBal_1_Req[1]
      </XPath>
      </TANRef>
    </OneTimePassword>
  </RequestSigList>
  <Orders>
    <fintstrans:AcctBal 1 Req
      xmlns:fintstrans="http://www.fints.org/spec/xmlschema/4.0/final/transactions"
      ...
    </fintstrans:AcctBal_1_Req>
  </Orders>
</RequestList>
```

IV.4.3 Benutzerdefinierte Signatur

Eine benutzerdefinierte Signatur enthält keine im Rahmen des FinTS-Standards spezifizierten Referenzierungen. Die Belegung ist somit identisch bei der Verwendung als Boten- oder Auftragssignatur.

Eine benutzerdefinierte Auftragssignatur signiert in einer Benutzernachricht implizit alle Aufträge einer *RequestList* bzw. in einer Kreditinstitutsnachricht alle Rückmeldungen zur Auftragsliste sowie alle Antworten in einer *ResponseList*.

| | | |
|---------------|----------------------|--|
| Kapitel: V | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 130 | Stand: 09.07.2004 | Kapitel: Verschlüsselte und komprimierte Nachrichtenteile Abschnitt: Auftragssignatur |

V. VERSCHLÜSSELTE UND KOMPRIMIERTE NACHRICHTENTEILE

| | | |
|------------|--|------------|
| V.1 | Aufbau des Verschlüsselungssegments | 131 |
| V.2 | Verschlüsselung des Nachrichtenkörpers | 134 |
| V.3 | Verschlüsselung von Aufträgen und Auftragsantworten | 135 |
| V.4 | Komprimierung | 136 |

V.1 Aufbau des Verschlüsselungssegments

FinTS-Nachrichten können auf zwei Nachrichtenebenen verschlüsselt werden. Zur Darstellung der Verschlüsselung in XML wird der [XML Encryption] Standard des W3C verwendet. Verschlüsselung ist nur im Sicherheitsverfahren [HBCI] möglich (siehe auch [HBCI], Abschnitt II.5.2 Verschlüsselungsdaten).

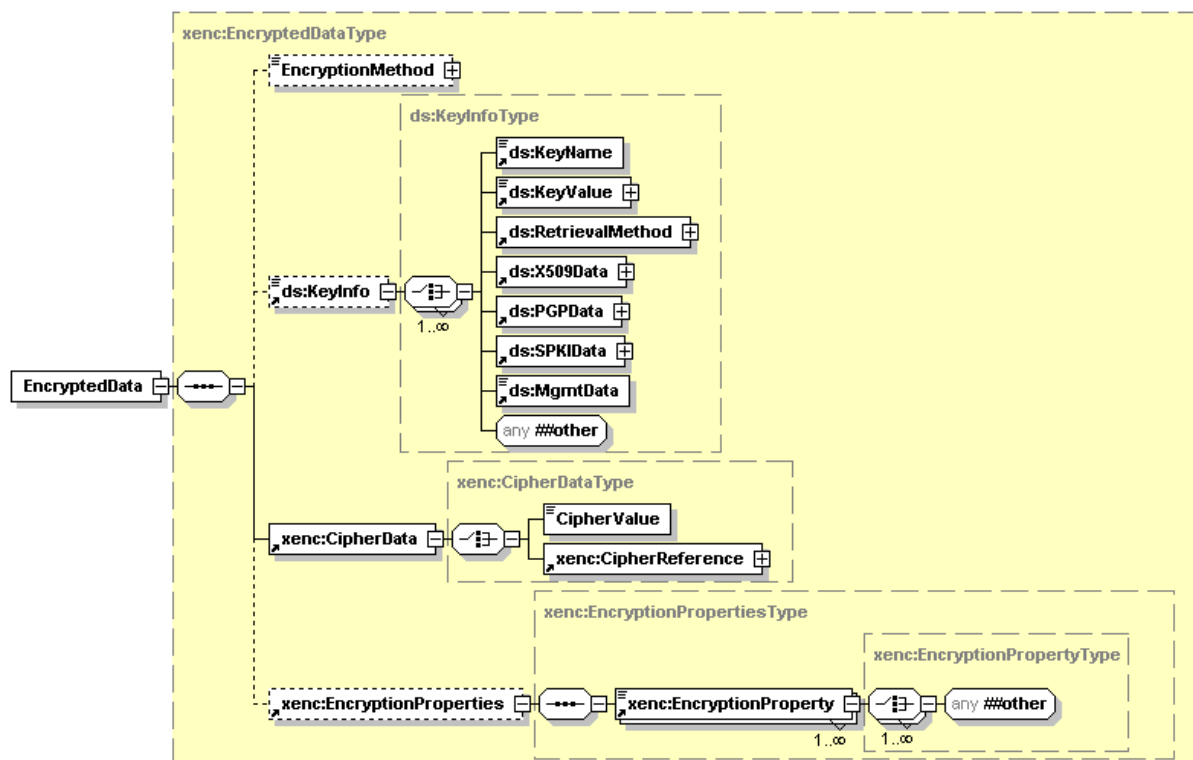


Abbildung 133: Verschlüsselung mit dem EncryptedData-Element

Die Abbildung zeigt das Element *EncryptedData*, welches die nach XML Encryption verschlüsselten Teile einer FinTS-Nachricht enthält.

♦ Verfahren zur Nachrichtenverschlüsselung

Das Attribut *Algorithm* des Elements *EncryptionMethod* enthält die Beschreibung des Verfahrens zur Verschlüsselung der Nachrichteninhalte. Die zulässigen Verfahren zur Nachrichtenverschlüsselung sind durch die Sicherheitsprofile des Sicherheitsverfahrens [HBCI] festgelegt (siehe [HBCI], Abschnitt II.1.1 Sicherheitsprofile). Das Attribut *Type* des *EncryptedData*-Elements muss bei Verschlüsselung in FinTS immer mit dem Wert <http://www.w3.org/2001/04/xmlenc#Element> belegt werden.

Unterhalb des Elements *EncryptionProperty* wird das aktuelle Sicherheitsprofil übertragen. Hier ist bei Verwendung des RDH-Verfahrens das Element *RDH*, bei Verwendung des DDV-Verfahrens das Element *DDV* jeweils mit dem entsprechenden Variantenbezeichner einzustellen. Ein Benutzer oder Kreditinstitut hat alle Signaturen oder Verschlüsselungen in einem Dokument im selben Sicherheitsprofil vorzunehmen.

| | | | | |
|----------|-----|------------|-------------------------------------|---|
| Kapitel: | V | Version: | 4.0 | Financial Transaction Services (FinTS) |
| | | Dokument: | XML-Syntax | |
| Seite: | 132 | Stand: | 09.07.2004 | Kapitel: Verschlüsselte und komprimierte Nachrichtenteile |
| | | Abschnitt: | Aufbau des Verschlüsselungssegments | |

◆ Verschlüsselter Nachrichteninhalt

Der verschlüsselte Teil der Nachricht befindet sich in dem Element *CipherValue* unter dem Element *CipherData*. Der Inhalt von *CipherValue* wird durch Anwendung des Verschlüsselungsalgorithmus aus *EncryptionMethod* und des Sitzungsschlüssels (siehe folgender Absatz) auf die zu verschlüsselnden Daten berechnet. Er wird in *base64*-Codierung eingestellt. Diese Daten müssen vor der Verschlüsselung mit dem Algorithmus [Canonical XML] kanonisiert werden. Das *CipherReference*-Element und die *EncryptionProperties* werden in FinTS nicht zur Verschlüsselung benutzt.

◆ Verschlüsselter Sitzungsschlüssel

Da es sich bei den Verschlüsselungen im Sicherheitsverfahren [HBCI] immer um zweistufige Verfahren handelt, enthält das Element *KeyInfo* den zur Nachrichtenverschlüsselung verwendeten Schlüssel (Sitzungsschlüssel) nicht direkt, sondern in verschlüsselter Form als *EncryptedKey*-Element. Dieses wiederum enthält ein Element *EncryptionMethod* mit der Beschreibung des Verfahrens zur Verschlüsselung des Sitzungsschlüssels gemäß den Sicherheitsprofilen des Sicherheitsverfahrens [HBCI], Abschnitt II.1.1 *Sicherheitsprofile*. Außerdem enthält es den verschlüsselten DES-Sitzungsschlüssel im *CipherData*-Element sowie die Daten des zu seiner Verschlüsselung verwendeten DES- bzw. RDH-Schlüssels in Form eines *DDVKeyInfo* (Schlüsselinformationen für das Sicherheitsverfahren DDV) bzw. *RDHKeyInfo* (Schlüsselinformationen für das Sicherheitsverfahren RDH) im *KeyInfo*-Element.

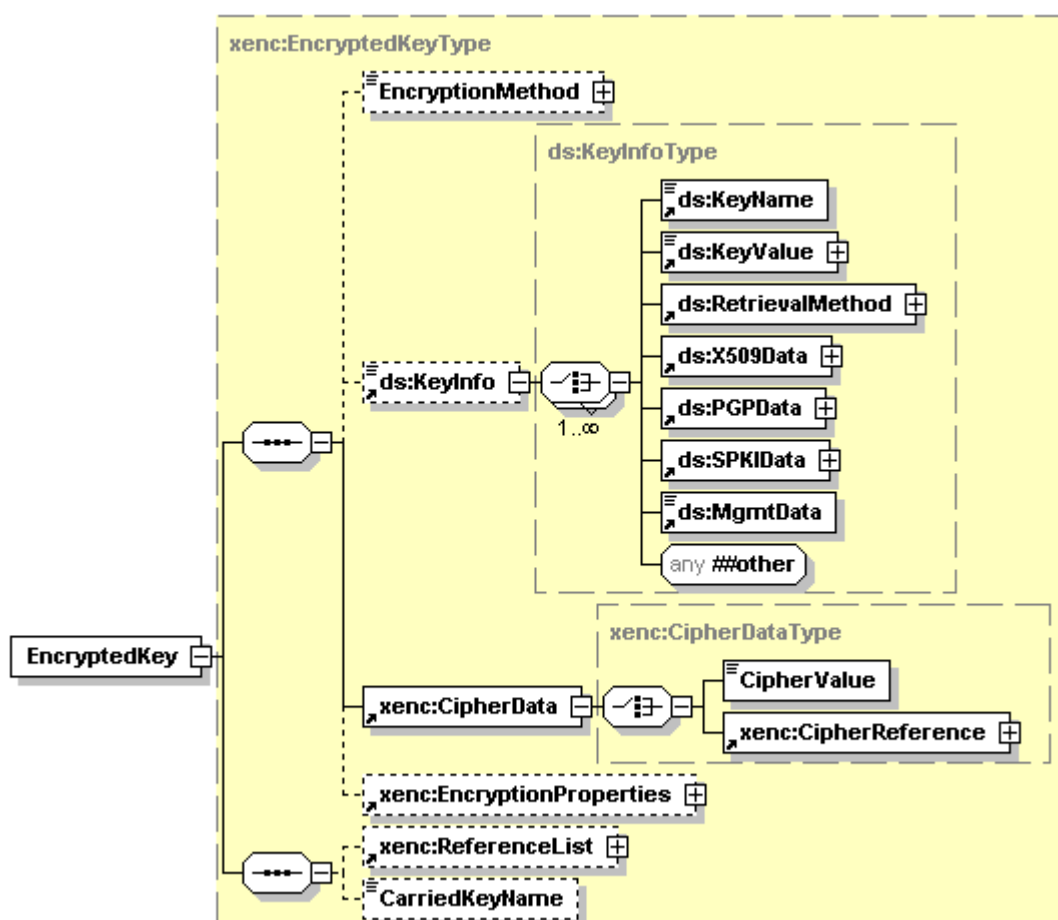


Abbildung 134: Verschlüsselter Sitzungsschlüssel

| | | |
|---|----------------------|---------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: V |
| Kapitel: Verschlüsselte und komprimierte Nachrichtenteile Abschnitt: Aufbau des Verschlüsselungssegments | Stand: 09.07.2004 | Seite: 133 |

Schlüsselinformationen für das Sicherheitsverfahren DDV

In Benutzernachrichten wird der **Benutzerschlüsselname** belegt, in Kreditinstitutsnachrichten hingegen der **Kreditinstitutsschlüsselname**.

Das Element Feld **Kartenidentifizierung** wird in Kreditinstitutsnachrichten leer gelassen.

Obwohl im DDV-Verfahren keine unterschiedlichen Schlüssel existieren, wird das Element **Typ** wie im RDH-Verfahren mit dem logischen Typ des für die jeweilige Operation notwendigen Schlüssels belegt, hier 'C' für Chiffrierschlüssel.

Schlüsselinformationen für das Sicherheitsverfahren RDH

In Benutzernachrichten wird der **Benutzerschlüsselname** belegt, in Kreditinstitutsnachrichten hingegen der **Kreditinstitutsschlüsselname**.

Das Beispiel zeigt den Inhalt des Elements *ReqMsg* nach der Verschlüsselung des *ReqMsgBody*-Elements. Das Element *ReqMsgBody* wurde nach der Verschlüsselung durch das Element *EncryptedData* ersetzt.

```
<ReqMsg xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <ReqMsgHeader>
    <BankID>
      <CountryCode>280</CountryCode>
      <BankCode>99950001</BankCode>
    </BankID>
    <UserRef>USER_REF12345</UserRef>
    <UserTextRef>MeineReferenz</UserTextRef>
    <MsgNo>1</MsgNo>
  </ReqMsgHeader>
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Type="http://www.w3.org/2001/04/xmlenc#Element">
    <xenc:EncryptionMethod
      Algorithm="http://www.fints.org/spec/xmlschema/4.0/final/xmlenc#two-key-
      tripledesh-cbc-isol0126"/>
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <xenc:EncryptedKey>
        <xenc:EncryptionMethod Algorithm="http://www.w3c.org/2001/04/xmlenc#rsa"/>
        <ds:KeyInfo>
          <RDHKeyInfo>
            <BankKeyName>
              <BankID>
                <CountryCode>280</CountryCode>
                <BankCode>99950001</BankCode>
              </BankID>
              <Number>1</Number>
              <Version>1</Version>
              <Type>C</Type>
            </BankKeyName>
          </RDHKeyInfo>
        </ds:KeyInfo>
      <xenc:CipherData>
        <xenc:CipherValue>DEADBEEF...S9B4MHbzwD9/auK</xenc:CipherValue>
      </xenc:CipherData>
    </xenc:EncryptedKey>
  </ds:KeyInfo>
  <xenc:CipherData>
    <xenc:CipherValue>DEADBEEF...404r7NX4F2uil</xenc:CipherValue>
  </xenc:CipherData>
  <xenc:EncryptionProperties>
    <xenc:EncryptionProperty>
      <RDH><Option>1</Option></RDH>
    </xenc:EncryptionProperty>
  </xenc:EncryptionProperties>
  </xenc:EncryptedData>
</ReqMsg>
```

| | | |
|---------------|----------------------|--|
| Kapitel: V | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 134 | Stand: 09.07.2004 | Kapitel: Verschlüsselte und komprimierte Nachrichtenteile Abschnitt: Verschlüsselung des Nachrichtenkörpers |

V.2 Verschlüsselung des Nachrichtenkörpers

Bei der Verschlüsselung des Nachrichtenkörpers wird der gesamte Teilbaum unter dem Wurzelement des Nachrichtenkörpers (*ReqMsgBody* bzw. *RespMsgBody*) verschlüsselt und durch das *EncryptedData*-Element ersetzt. Bei der Entschlüsselung ist entsprechend das *EncryptedData*-Element durch den entschlüsselten Teilbaum zu ersetzen.

Eine erneute Verschlüsselung des verschlüsselten Teils (*super encryption*) ist in FinTS nicht zulässig, allerdings ist die Komprimierung formal auch eine [XML Encryption], siehe *V.4 Komprimierung*.

Die beiden folgenden Abbildungen zeigen den Teil des Nachrichtenaufbaus zur Verschlüsselung der Nachrichtenkörper einer Benutzernachricht und einer Kreditinstitutsnachricht.

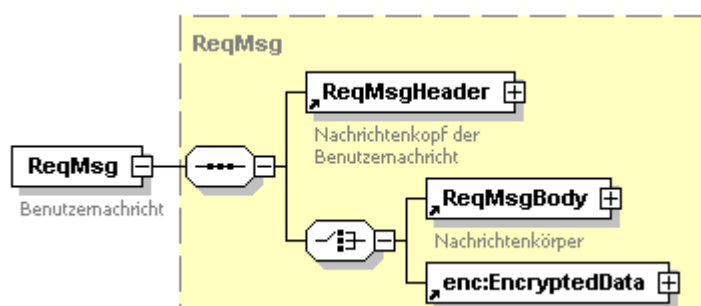


Abbildung 135: Verschlüsselung des Nachrichtenkörpers der Benutzernachricht

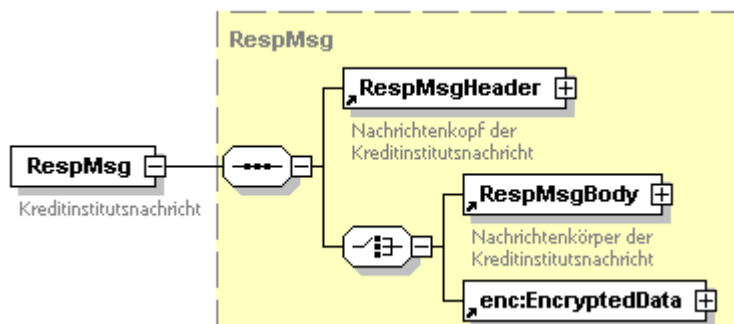


Abbildung 136: Verschlüsselung des Nachrichtenkörpers der Kreditinstitutsnachricht

| | | |
|---|-------------------|------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: V |
| Kapitel: Verschlüsselte und komprimierte Nachrichtenteile Abschnitt: Verschlüsselung von Aufträgen und Auftragsantworten | Stand: 09.07.2004 | Seite: 135 |

V.3 Verschlüsselung von Aufträgen und Auftragsantworten

Die Verschlüsselung von Aufträgen und Auftragsantworten ist nur für bestimmte Nachrichtentypen zulässig (siehe auch *III.3 Verschiedene Benutzer- und Antwortnachrichten* und *III.4 Keymanagement-Nachrichten*). Verschlüsselt wird jeweils der gesamte Teilbaum der *RequestList* bzw. *ResponseList*, das *EncryptedData*-Element ersetzt nach der Verschlüsselung den verschlüsselten Teilbaum. Umgekehrt wird bei der Entschlüsselung *EncryptedData* wieder durch den entschlüsselten Teilbaum ersetzt.

Eine erneute Verschlüsselung des verschlüsselten Teils *super encryption* ist in FinTS nicht zulässig, allerdings ist die Komprimierung formal auch eine [XML Encryption] (siehe *V.4 Komprimierung*).

Die normale Benutzernachricht *StandardReq* bzw. ihre Antwort *StandardResp* können mehrere Auftrags- bzw. Antwortteile enthalten. Dabei können verschlüsselte und unverschlüsselte Teile beliebig gemischt werden (vgl. Abbildung 137 und Abbildung 138).

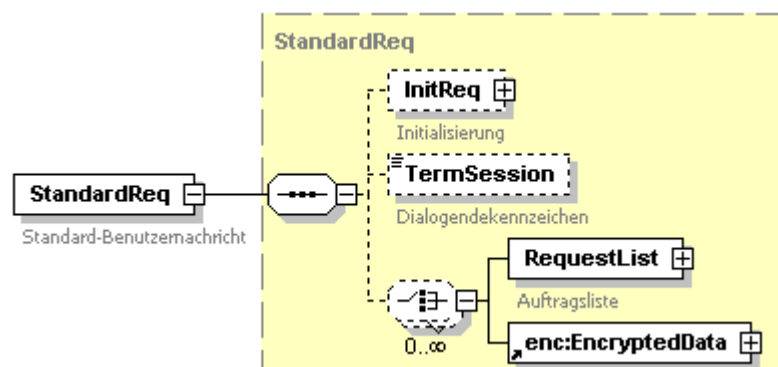


Abbildung 137: Auftragsverschlüsselung in der Standard-Benutzernachricht

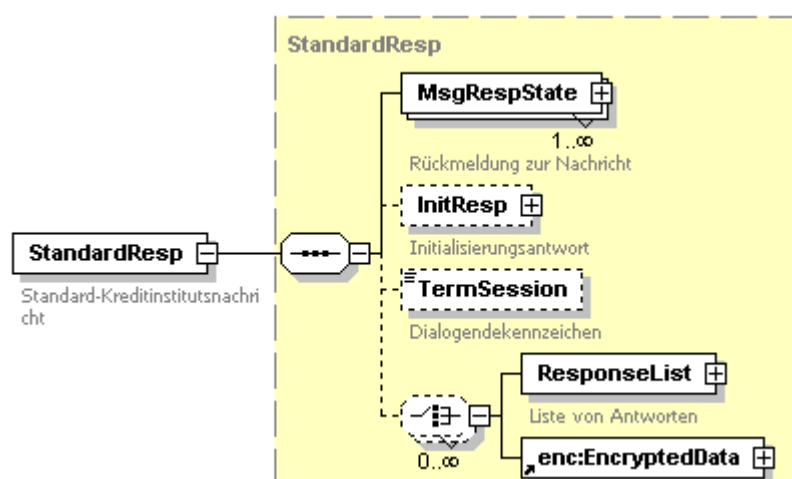


Abbildung 138: Auftragsverschlüsselung in der Standard-Kreditinstitutsnachricht

| | | |
|---------------|----------------------|---|
| Kapitel: V | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 136 | Stand: 09.07.2004 | Kapitel: Verschlüsselte und komprimierte Nachrichtenteile Abschnitt: Komprimierung |

V.4 Komprimierung

Alle Teile einer FinTS-Nachricht, für die die Syntax eine Verschlüsselung erlaubt, können optional komprimiert werden. Die Komprimierung ist also mit allen Typen von Signaturen, mit verschlüsselten oder unverschlüsselten Nachrichten und auch mit anonymen Nachrichten kombinierbar. In FinTS wird die XML-Kompression als eine spezielle Form der Verschlüsselung behandelt. Daher wird analog zur Verschlüsselung der [XML Encryption]-Standard verwendet.

Bei der Komprimierung ersetzt das *EncryptedData*-Element die komprimierten Nachrichtenteile. Das Attribut *Type* des *EncryptedData*-Elements ist mit dem Wert <http://www.w3.org/2001/04/xmlenc#Element> zu belegen. Das Attribut *Algorithm* gibt das verwendete Komprimierungsverfahren (im Beispiel [RFC1951]) an. Die möglichen Komprimierungsverfahren werden durch das Profil des verwendeten Sicherheitsverfahrens, [HBCI] bzw. [PINTAN], festgelegt. Die, von einem Kreditinstitut unterstützten Komprimierungsverfahren, werden innerhalb der Bankparameterdaten übermittelt. Der komprimierte Teil wird in *base64*-Codierung im Element *CipherValue* abgelegt. Die Elemente *KeyInfo* und *EncryptionProperties* sind nicht vorhanden.

Beispiel:

```
<EncryptedData
  xmlns="http://www.w3.org/2001/04/xmlenc#"
  Type='http://www.w3.org/2001/04/xmlenc#Element'>
  <EncryptionMethod
    Algorithm="http://www.fints.org/spec/xmlschema/4.0/final/xmlcomp#rfc1951"/>
    <CipherData>
      <CipherValue>DEADBEEFK...VLVLZVL</CipherValue>
    </CipherData>
  </EncryptionMethod>
</EncryptedData>
```

Wenn FinTS-Nachrichtenteile komprimiert und verschlüsselt übertragen werden, sind sie immer zuerst zu komprimieren und danach zu verschlüsseln. Auf der Empfängerseite müssen sie dann erst entschlüsselt und anschließend dekomprimiert werden. Das *EncryptedData*-Element der Verschlüsselung ersetzt dann das *EncryptedData*-Element des komprimierten Nachrichtenteils.

Die mehrfache Verschlüsselung von XML-Fragmenten wird in [XML Encryption] als *super-Encryption* bezeichnet. In FinTS ist keine mehrfache Verschlüsselung zulässig, es sei denn, es handelt sich um eine Komprimierung gefolgt von einer Verschlüsselung.

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VI |
| Kapitel: WEBSERVICES Abschnitt: Komprimierung | Stand: 09.07.2004 | Seite: 137 |

VI. WEBSERVICES

| | |
|-------------------------------|------------|
| VI.1 Webservices | 138 |
| VI.1.1 Einleitung..... | 138 |
| VI.1.2 SOAP | 140 |
| VI.1.3 WSDL | 142 |

| | | |
|----------------|----------------------|--|
| Kapitel: VI | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 138 | Stand: 09.07.2004 | Kapitel: WEBSERVICES Abschnitt: Webservices |

VI.1 Webservices

VI.1.1 Einleitung

FinTS-Anwendungen können mit Webservices implementiert werden. Webservices sind elektronische Dienste, die durch den Austausch von XML-Dokumenten basierend auf Internet-Protokollen erbracht werden.

Die folgende Abbildung verdeutlicht dies anhand eines Beispiels. Im Beispiel werden FinTS-Nachrichten zwischen einem Benutzer und einem Kreditinstitut ausgetauscht (3). Der Datenaustausch erfolgt synchron und direkt (ohne Intermediäre). Dazu ruft eine Anwendung des Benutzers (Requestor Agent) den Webservice des Kreditinstituts (Provider Agent) auf (2). Zur Implementierung werden gemeinsame Zusicherungen genutzt (1), damit beide Anwendungen miteinander kommunizieren können. Die Zusicherungen legen sowohl die Schnittstelle des Webservices (WSD) als auch die Semantik der ausgetauschten Nachrichten fest.

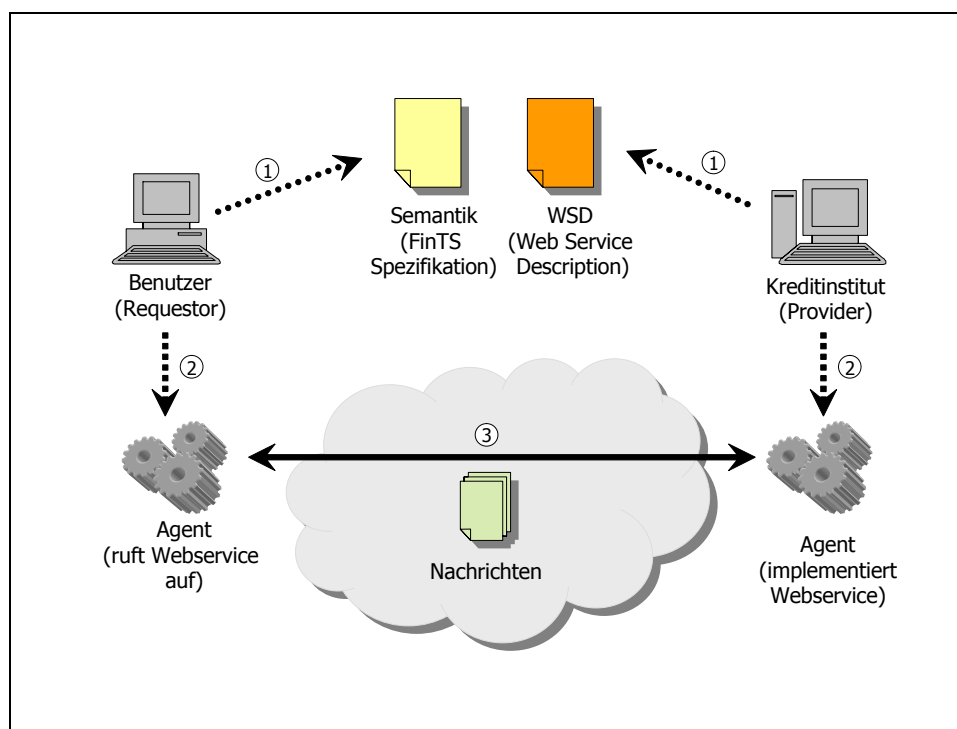


Abbildung 139: WebService Beispiel

Die Spezifikation von FinTS bestimmt die Semantik des Webservices. Die Semantik wird durch die entsprechende Anwendungslogik der Webservices implementiert. Ergänzend dazu enthält die Web Service Description (WSD) eine Schnittstellenbeschreibung, die automatisiert verarbeitet werden kann.

Die vom W3C normierten Webservice-Standards unterstützen vielfältige Übertragungsformen. In FinTS wird nur ein Teil davon genutzt. Das Schichtenmodell für Webservices zeigt, dass sich die Sicherheitsmethoden unabhängig zu den Webservice-Schichten verhalten. Weder SSL noch die Sicherheitsstandards für XML (XML Signature und XML Encryption) werden durch die Webservice-Standards

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VI |
| Kapitel: WEBSERVICES Abschnitt: Webservices | Stand: 09.07.2004 | Seite: 139 |

beeinflusst. Die unterste Schicht eines Webservices ist die Kommunikationsschicht. In ihr wird das Übertragungsprotokoll für die XML-Dokumente festgelegt. In FinTS werden die Nachrichten per SMTP oder HTTP übertragen. Die Nachrichten von FinTS werden in die Nachrichten des XML Protokolls SOAP eingebettet ([SOAP 1], [SOAP 2]). Auf der beschreibenden Ebene wird die Webservice-Schnittstelle mit der Webservice Description Language WSDL ([WSDL 1, WSDL 2, WSDL 3]) festgelegt. Alle Standards über der Kommunikationsebene basieren auf den XML-Standards XML 1.0, Namensräume und XML Schema.

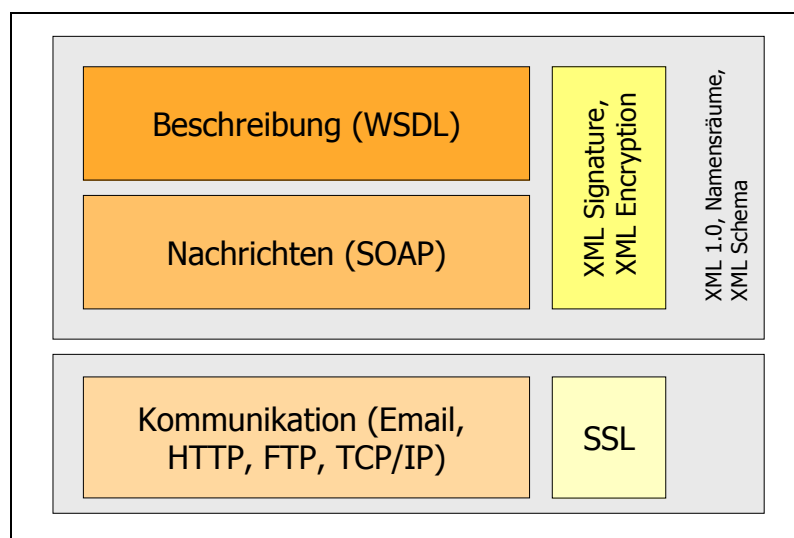


Abbildung 140: Webservice Schichtenmodell

In den beiden folgenden Abschnitten wird die Verwendung der Standards SOAP und WSDL in FinTS genauer beschrieben. Um Missverständnisse zu vermeiden, werden zuvor noch einige Begriffe aus FinTS mit der Terminologie von Webservices verglichen.

◆ Node

Ein Knoten (Node) in einer Webservice-Architektur ist eine Entität, die am Datenaustausch mit Webservices teilnimmt. In FinTS entspricht ein Knoten dem SOAP-Prozessor eines Kunden, eines Kreditinstituts oder eines Intermediärs. Der SOAP-Prozessor ist implementiert das SOAP-Protokoll.

◆ Endpoint

Ein Endpoint ist die Assoziation zwischen einer Lokation (Netzwerkadresse) und einem Binding. Die Netzwerkadressen von Webservices werden in FinTS durch URIs festgelegt.

◆ Binding

Ein Binding ordnet einer Schnittstelle ein bestimmtes Protokoll zu. HTTP wird derzeit als einziges Protokoll für FinTS zugelassen, weil die übrigen Protokoll-Bindings für SOAP nicht ausreichend durch das W3C normiert sind.

| | | |
|----------------|----------------------|--|
| Kapitel: VI | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 140 | Stand: 09.07.2004 | Kapitel: WEBSERVICES Abschnitt: Webservices |

◆ **Interface**

In FinTS existieren verschiedene Operationen für die synchrone und asynchrone Kommunikation. Die Schnittstellen-Beschreibung (Interface) ordnet jeder Operation einen Datentyp zu.

◆ **Gateway**

Gemäß der [Formals] können Intermediäre FinTS-Nachrichten verändern (z. B. eine Signatur einfügen). Dadurch unterscheidet sich der Begriff Intermediär in FinTS von dem in Begriff Intermediär im Kontext von Webservices. Ein Intermediär-Webservice darf die Nachrichtenkörper der empfangenen Nachrichten nicht verändern. Wenn ein Webservice bei Weiterleiten die Nachrichtenkörper manipuliert, spricht man in einer Webservice-Architektur von einem Gateway.

◆ **Message Exchange Patterns (MEPs)**

Die Kommunikationsformen direkte Kommunikation versus Kommunikation über einen Intermediär und synchrone versus asynchrone Kommunikation decken sich nicht mit den sogenannten Message Exchange Patterns, die durch das W3C normiert wurden. Wenn FinTS-Nachrichten in SOAP ausgetauscht werden, erfolgt dies immer nach dem Request/Response MEP, sowohl bei der synchronen als auch bei der asynchronen Kommunikation.

◆ **WSDL**

Die Webservice Description Language war bei der Spezifikation von FinTS 4.0 nicht abschließend durch das W3C normiert. Daher kann lediglich empfohlen werden, WSDL-Beschreibungen zu FinTS-Webservices zu publizieren, ohne eine konkrete Syntax vorzugeben.

VI.1.2 SOAP

Das SOAP Protokoll definiert den XML-basierten Datenaustausch in einer verteilten Umgebung. SOAP ist wie HTTP ein zustandsloses Protokoll. Für den Datenaustausch werden im SOAP-Standard verschiedene Message Exchange Patterns (MEPs) definiert. In FinTS muss das Request-Response MEP für alle Arten des Datenaustauschs benutzt werden. Für den Datenaustausch mit SOAP ist ausschließlich das HTTP-Protokoll zulässig. Die SOAP-Nachrichten müssen mit dem HTTP POST-Verfahren übertragen werden.

Bei der synchronen Kommunikation enthält der SOAP-Request eine FinTS-Benutzernachricht, die durch eine in den SOAP-Response eingebettete FinTS-Kreditinstitutsnachricht erwidert werden muss. Bei der asynchronen Kommunikation wird eine FinTS-Nachricht (Benutzernachricht oder Kreditinstitutsnachricht) als SOAP-Request verschickt. Der SOAP-Response enthält keine FinTS-Nachricht. Im SOAP-Response kann allerdings ein SOAP-Fault Element enthalten sein, um SOAP-spezifische Kommunikationsfehler zu melden. SOAP-Nachrichten, die zum Austausch von FinTS-Nachrichten versendet werden, dürfen SOAP-Fault-Elemente enthalten. Die Verwendung von SOAP-Faults wird durch FinTS jedoch nicht spezifiziert. Alle in FinTS beschriebenen Fehler müssen beim Einsatz des SOAP-Protokolls analog zu den anderen Protokollen innerhalb der FinTS-Nachrichten übermittelt werden.

Beim asynchronen Verfahren existieren auf beiden SOAP-Knoten (Sender und Empfänger) Webservices, die mit SOAP Engines implementiert wurden. Beim synchronen Verfahren muss lediglich auf der Empfängerseite ein Webservice

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VI |
| Kapitel: WEBSERVICES Abschnitt: Webservices | Stand: 09.07.2004 | Seite: 141 |

implementiert werden. Für das asynchrone Verfahren muss dem Kreditinstitut bzw. dem Intermediär der URI des Empfänger-Webservice mitgeteilt werden.

Die folgende Abbildung zeigt den Aufbau einer SOAP-Nachricht, die eine FinTS-Nachricht enthält. Der Nachrichten-Umschlag (SOAP Envelope) enthält ein SOAP Header Element und ein SOAP Body Element. Die Übertragung des SOAP Header Elements ist in FinTS mit einer Ausnahme obligatorisch, weil dieses Element den Nachrichtenkopf der FinTS-Nachricht enthält. Im asynchronen Übertragungsverfahren ist im SOAP-Response keine FinTS-Nachricht enthalten, deshalb kann das SOAP Header Element entfallen. Analog zum SOAP Header muss der SOAP Body den Nachrichtenkörper der FinTS-Nachricht enthalten. Die Ausnahme ist auch hier wieder der SOAP-Response im asynchronen Verfahren. Das Wurzelement der FinTS-Nachricht (ReqMsg bzw. RespMsg) entfällt.

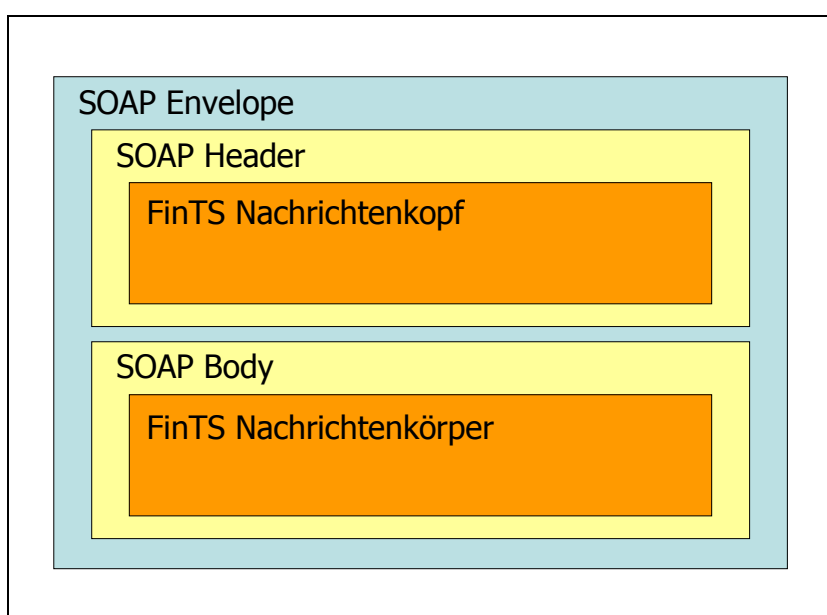


Abbildung 141: Transport einer FinTS-Nachricht mit SOAP

SOAP unterstützt zwei Arten des Nachrichtenaustauschs. Den sogenannten Dokument-orientierten Austausch und die Remote Procedure Calls (RPCs). FinTS-Nachrichten müssen im Dokument-orientierten Verfahren ausgetauscht werden. Bei diesem Verfahren enthalten die SOAP-Nachrichten XML-basierte Inhalte, die durch ein XML Schema typisiert werden.

SOAP-Nachrichten können zum Transport mit SSL verschlüsselt werden. Für die SSL-Verschlüsselung gilt analog zu den Transportmedien-spezifischen Festlegungen für HTTP, dass mindestens die SSL-Version 3.0 zu verwenden ist und dass die SSL-Verschlüsselung die HBCI-Verschlüsselung ersetzen kann.

In FinTS sind nur konforme SOAP-Engines zur SOAP Version 1.2 zulässig.

| | | |
|----------------|----------------------|--|
| Kapitel: VI | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 142 | Stand: 09.07.2004 | Kapitel: WEBSERVICES Abschnitt: Webservices |

Das folgende Beispiel zeigt eine FinTS-Auftragsnachricht, die in einer SOAP-Nachricht transportiert wird.

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"
  xmlns="http://www.fints.org/spec/xmlschema/4.0/final/types"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  env:encodingStyle="http://www.w3.org/2003/05/soap-encoding">
  <env:Header env:encodingStyle="http://www.w3.org/2003/05/soap-encoding">
    <ReqMsgHeader xsi:schemaLocation=
      "http://www.fints.org/spec/xmlschema/4.0/final/types
      http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd">
      ...
    </ReqMsgHeader>
  </env:Header>
  <env:Body env:encodingStyle="http://www.w3.org/2003/05/soap-encoding">
    <ReqMsgBody "http://www.fints.org/spec/xmlschema/4.0/final/types
      http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd">
      ...
    </ReqMsgBody>
  </env:Body>
</env:Envelope>
```

Die Elemente der SOAP-Nachricht sind im SOAP-Namensraum definiert (<http://www.w3.org/2003/05/soap-envelope>). Der default-Namensraum enthält den URI der FinTS-Version 4.0 (<http://www.fints.org/spec/xmlschema/4.0/final/types>). Die Namensraumdeklarationen des Namensraumes für FinTS-Nachrichten und die Namensraumdeklaration für XML Schemainstanzen (<http://www.w3.org/2001/XMLSchema-instance>) im SOAP-Envelope vermeiden, dass die Deklarationen im Nachrichtenkopf und im Nachrichtenkörper der FinTS-Nachricht mehrfach angegeben werden müssen. Das Attribut *encodingStyle* legt fest, dass der Inhalte der SOAP-Elemente gemäß der SOAP-Encodingregeln kodiert ist. Das *schemaLocation*-Attribut enthält den Namensraum-URI für FinTS-Typen und den URI für das zugehörige Schema *message.xsd*.

Die Aufspaltung der FinTS-Nachrichten in Nachrichtenkopf und Nachrichtenkörper ist nur zum Zweck des Transports zulässig. (Sie hat in SOAP-Nachrichten die Auswirkung, dass die in den Nachrichten verwendeten XPath-Referenzen nicht mehr korrekt sind.) Die beiden FinTS-Nachrichtenteile sind zur weiteren Verarbeitung wieder in die Ursprungsform zu überführen, in der die beiden Nachrichtenteile vom entsprechenden Wurzelement umschlossen werden.

VI.1.3 WSDL

Die Webservice Description Language WSDL ist eine Schnittstellen-Beschreibung (ähnlich einer IDL) für die Dienste, die durch einen Webservice angeboten werden. Darüber hinaus werden in WSDL die Protokoll-Bindungen für das Protokoll definiert, auf dem ein Webservice basiert. Prinzipiell ist eine WSDL-Beschreibung für einen Webservice nicht erforderlich, um z. B. mittels SOAP FinTS-Nachrichten auszutauschen.

Da in der aktuellen FinTS-Version nur eine bestimmte Form des HTTP-Bindings mit einem einzigen Message Exchange Pattern zulässig ist, kann auf die WSDL-Beschreibung verzichtet werden.

Eine WSDL-Beschreibung kann für das Web Service Discovery genutzt werden. Das heißt, ein Kreditinstitut kann die WSDL-Beschreibung seines Webservices in zentralen Repositories veröffentlichen. Dazu existieren weiterführende XML Vokabulare (z. B. UDDI und WSIL), die das automatisierte Auffinden von Webservices unterstützen.

Eine WSDL Beschreibung kann außerdem dazu genutzt werden, um dem Kreditinstitut bei der asynchronen Kommunikation die WSDL-Beschreibung des Empfängers zu übermitteln.

| | | |
|--|----------------------|----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VI |
| Kapitel: WEBSERVICES Abschnitt: Webservices | Stand: 09.07.2004 | Seite: 143 |

Die Webservice Description Language WSDL wurde zum Erstellungszeitpunkt der vorliegenden FinTS-Version noch nicht abschließend spezifiziert. Deshalb wird in diesem Abschnitt nur ein Beispiel für den Einsatz von WSDL gegeben. Das Beispiel basiert auf den zum Erstellungszeitpunkt aktuellen Working Drafts des W3C. Die WSDL-Beschreibung wird sich voraussichtlich noch bis zur abschließenden Spezifikation als Recommendation ändern.

Das Beispiel zeigt eine WSDL-Datei, die einen FinTS-Webservice definiert. Die Definitionen befinden sich im *targetNamespace* des URI für die FinTS-Version 4.0. Durch die Angabe des *targetNamespace*-Attributs wird der Webservice eindeutig als FinTS-Webservice spezifiziert. Das *import*-Element inkludiert die FinTS-Datentypen in die WSDL-Datei. Die Nachrichten, die mit dem Webservice ausgetauscht werden, sind durch die *message*-Elemente gekennzeichnet. Sie enthalten die Nachrichtenköpfe bzw. Nachrichtenkörper der entsprechenden FinTS-Nachrichten.

```
<definitions targetNamespace="http://www.fints.org/spec/xmlschema/4.0/final"
  xmlns="http://www.w3.org/2003/03/wsd1"
  xmlns:tns="http://www.xy-bank.de/webservices/fints"
  xmlns:wssoap="http://www.w3.org/2003/06/wsd1/soap12"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:fintstype="http://www.fints.org/spec/xmlschema/4.0/final/types">
  <xs:import namespace=
    "http://www.fints.org/spec/xmlschema/4.0/final/types"
    schemaLocation=
    "http://www.fints.org/spec/xmlschema/4.0/final/types/message.xsd"/>
  <message name="ReqMsg">
    <part name="ReqMsgHeader" type="fintstype:ReqMsgHeader"/>
    <part name="ReqMsgBody" type="fintstype:ReqMsgBody"/>
  </message>
  <message name="RespMsg">
    <part name="RespMsgHeader" type="fintstype:RespMsgHeader"/>
    <part name="RespMsgBody" type="fintstype:RespMsgBody"/>
  </message>
  <interface name="FinTSInterface">
    <operation name="OneWay">
      <input message="ReqMsg"/>
      <output message="RespMsg"/>
    </operation>
    <operation name="RequestResponse">
      <input message="ReqMsg"/>
      <output message="RespMsg"/>
    </operation>
  </interface>
  <binding name="FinTSSOAPBinding" interface="FinTSInterface">
    <wssoap:binding protocol=
      "http://www.w3.org/2003/05/soap/bindings/HTTP/"
      styleDefault="document"
      encodingStyleDefault="http://www.w3.org/2003/05/soap-encoding"/>
    <operation name="OneWay">
      <pattern="http://www.w3.org/2003/11/wsd1/in-out">
      <wssoap:operation soapAction=
        "http://www.xy-bank.de/webservices/fints/oneWay"/>
      </operation>
    <operation name="RequestResponse">
      <pattern="http://www.w3.org/2003/11/wsd1/in-out">
      <wssoap:operation soapAction=
        "http://www.xy-bank.de/webservices/fints/requestresponse"/>
      </operation>
    </binding>
    <service name="FinTSService" interface="FinTSInterface">
      <endpoint name="SOAP" binding="FinTSSOAPBinding"/>
    </service>
  </definitions>
```

Die Knoten in einem FinTS-Netzwerk repräsentieren die Systeme von Kunden, Boten und Kreditinstituten. Die Knoten werden durch Eingangs- und Ausgangsnachrichten (*input/output*) einer Operation definiert. In FinTS-Implementierungen können mittels WSDL mehrere Datenaustauschverfahren zwischen diesen Knoten beschrieben werden. Die Verfahren OneWay und RequestResponse werden durch die jeweiligen Operationen (*operation*) in der

| | | |
|----------------|----------------------|--|
| Kapitel: VI | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 144 | Stand: 09.07.2004 | Kapitel: WEBSERVICES Abschnitt: Webservices |

Schnittstellenbeschreibung (*interface*) festgelegt. Das synchrone Verfahren von FinTS wird durch die Operation RequestResponse implementiert, das asynchrone Verfahren durch die Operation OneWay. Für die asynchrone Kommunikation könnte die Webservice-Beschreibung auf der Seite des Kunden eine Operation Notification enthalten, über die das Kundensystem asynchrone Nachrichten des Kreditinstituts empfängt.

Die SOAP-Bindings unter dem WSDL-Element *binding* bestimmen, wie SOAP benutzt wird, um die abstrakte Beschreibung der Schnittstelle umzusetzen. Das *protocol*-Attribut des *soap:binding*-Elements legt fest, dass das HTTP-Binding von SOAP genutzt wird.

Zu jeder Operation des Interfaces wird das Message Exchange Pattern RequestResponse durch den URI <http://www.w3.org/2003/11/wsdl/in-out> festgelegt. Allen Operationen werden ferner Action-URLs zugeordnet. Das sind die URLs, an die der HTTP-Request verschickt wird. Falls http mit SSL-Verschlüsselung eingesetzt wird, ändern sich die URLs entsprechend in *https://...*

Im *soapAction*-Attribut des Elements *soap:operation* wird der Wert für den HTTP SOAP Action Header festgelegt.

Im *service*-Element der WSDL-Beschreibung werden schließlich dem Endpoint des FinTS-Services sowohl das zuvor beschriebene Binding als auch eine Port-Adresse zugewiesen.

| | | |
|--|----------------------|-----------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VII |
| Kapitel: Anhang: Konventionen zur Bildung von Elementnamen Abschnitt: Webservices | Stand: 09.07.2004 | Seite: 145 |

VII. ANHANG: KONVENTIONEN ZUR BILDUNG VON ELEMENTNAMEN

Um eine homogene Namensgebung der XML-Deklarationen und -Definitionen zu erreichen, soll die Bildung der qualifizierenden Element- und Typnamen nach generellen Regeln erfolgen. Damit soll ein übergreifend einheitliches Verständnis des semantischen Inhalts von Namen sichergestellt werden.

1. Jedes Element erhält einen eindeutigen Namen aus dem [DataDictionary]. Der Name ist sinnvoll aus der englischsprachigen Bedeutung des Elements abzuleiten und ggf. abzukürzen.
2. Ein Element ist anhand des Namens eindeutig zu identifizieren, d. h. es existieren keine Homonyme.
3. Der Zeichenvorrat für die Bildung der Namen besteht aus den Zeichen A-Z, a-z, 0-9 und dem Unterstrich (_). Insbesondere enthält ein Element- oder Typname keine Leerzeichen.
4. Jedes Kürzel fängt mit einem groß geschriebenen alphabetischen Zeichen an. (Die Zeichenkette „XML“ ist in jeder Kombination von Groß- und Kleinschreibung am Anfang von qualifizierenden Namen verboten)
5. Qualifizierende Namen sind in XML *case sensitive*. Trotzdem dürfen sie nicht in verschiedenen case-sensitiven Schreibweisen verwendet werden. (Die Bedeutung der Elemente *AcctNr* und *acctnr* ist z. B. fachlich identisch, was zu Missverständnissen führen könnte, obwohl die Schreibweisen bei der XML-Verarbeitung unterscheidbar sind.)
6. Als Regel für die Reihenfolge der Kürzel gilt: Kürzel, die den Gegenstand bzw. das Wesen des Datenelements beschreiben, haben möglichst am Ende zu stehen. Kürzel, die dagegen nur beschreibende Funktion haben, werden voran gestellt. Wenn eines der folgenden Kürzel benutzt wird, sollte es das letzte Wort des Elementnamens bilden:
Acct, Amt, Code, Curr, Date, Id, Ref, Status

Beispiel:

| | |
|------------------------------|--------------------------|
| Minimum order amount | <i>MinOrderAmt</i> |
| Currency of exchange | <i>ExchCurr</i> |
| Identification of the party | <i>PartyId</i> |
| Portfolio required | <i>PortfolioRequired</i> |
| Type of denomination allowed | <i>DenomTypeAllowed</i> |

7. Artikel und Präpositionen (*of, in, the*) werden nicht im Elementnamen abgebildet.
8. Wenn Datenbeschreibungen aus XML-Fremdformaten (z. B. swiftML) verwendet werden, so werden die dort definierten Namen unverändert übernommen. (Die Fremdformate werden durch einen eigenen Namesraum gekennzeichnet, um Namenskollisionen zu vermeiden.)
9. Allgemein gebräuchliche Akronyme (z. B. ISIN, IBAN) werden stets in dieser Kurzform (alle Buchstaben groß geschrieben) verwendet, ansonsten sind Begriffe auszuschreiben.
10. Eigennamen werden nicht übersetzt.
11. Qualifizierende FinTS-Namen sollten 25 Stellen nicht überschreiten.

| | | |
|-----------------|----------------------|--|
| Kapitel: VII | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 146 | Stand: 09.07.2004 | Kapitel: Anhang: Konventionen zur Bildung von Elementnamen Abschnitt: Webservices |

12. Damit FinTS-Namen einheitliche und konsistente Namensbestandteile aufweisen, wird ein normierter englischer Wortschatz bei der Namensbildung herangezogen (s. Tabelle).¹

Beispiel: Das Adjektiv *allowed* wird bei gleicher Bedeutung anstelle von möglichen Alternativen wie *permissible*, *admissible*, *valid*, *in range* etc. verwendet.

Begriffe, die in der Liste nicht enthalten sind, werden aus der ausgeschriebenen bzw. sinnvoll abgekürzten, englischen Entsprechung gebildet.

| Deutscher Begriff | Englische Entsprechung | Standard-Kürzel |
|---------------------------------|--------------------------------|-----------------|
| Administration | administration | Admin |
| Adresse | address | Addr |
| Aktionär | stockholders | Stockh |
| alternativ, Alternative | alternative | Alt |
| änderbar | modifiable | Modif |
| Änderung | Modification | Mod |
| Anfrage | request | Req* |
| Angabe | specification | Spec |
| Anzahl | quantity | Qty* |
| ~aufdruck (z.B. Adressaufdruck) | printed | Print |
| ausführen, Ausführung | execute, execution | Exec |
| Auswahl | selection | Sel |
| Auszug (z.B. Konto~) | statement | Statemt |
| Bedingung | condition | Cond* |
| Begünstigter | beneficiary | Benef |
| Beschreibung | description | Desc* |
| Betrag | amount | Amt* |
| Börse | exchange | Exch |
| Code | code | Code |
| Datum | date | Date |
| Dokument | document | Doc |
| Durchschnitt, durchschnittlich | average | Avg* |
| Einzel~ (z.B. ~lastschrift) | single | Single |
| Einzelheiten | details | Details |
| Empfänger | beneficiary | Benef |
| erhältlich | available | Avail |
| erlaubt | allowed | Allowed |
| Erläuterung | remark | Rem |
| Fehler | error | Err |
| Finanz~ | financial | Fin* |
| Gesamt | total | Total |
| häufig, Häufigkeit | frequency | Freq* |
| Identifikation | ID, identifier, identification | Id* |

¹ Die mit einem Stern (*) gekennzeichneten Kürzel sind identisch mit den von SWIFT in [swiftML] vorgeschlagenen Abkürzungen.

| | | |
|--|-------------------|--------------|
| Financial Transaction Services (FinTS) Dokument: XML-Syntax | Version: 4.0 | Kapitel: VII |
| Kapitel: Anhang: Konventionen zur Bildung von Elementnamen Abschnitt: Webservices | Stand: 09.07.2004 | Seite: 147 |

| Deutscher Begriff | Englische Entsprechung | Standard-Kürzel |
|-----------------------------|----------------------------|-----------------|
| Information | information | Info* |
| Institut | institution | Inst |
| Instrument | instrument | Instr* |
| Kondition | condition | Cond |
| Konto | account | Acct* |
| Kennung | identifier, identification | Id |
| Kunde | customer | Cust |
| Kurs | price | Price |
| Länge | length | Len |
| Lastschrift | direct debit | DirDeb |
| Limit | limit | Lim |
| Liste | list | List |
| löschen, Löschung | delete, deletion | Del |
| maximal, Maximum | maximum | Max* |
| minimal, Minimum | minimum | Min* |
| möglich | possible | Possible |
| Name | name | Name |
| Nachricht | message | Msg |
| Nummer | number | No |
| Ort | place | Place |
| Parameter | parameter | Param |
| Partei | party | Party |
| Post~ (z.B. Postanschrift) | mailing | Mail |
| Post~ (z.B. Postleitzahl) | postal | Post |
| Produkt | product | Prod |
| Prozent | percentage | Pct* |
| Referenz | reference | Ref* |
| Rückmeldung | response | Resp |
| Saldo | balance | Bal |
| Sammel~ (z.B. ~überweisung) | multiple | Mult |
| Satz | record | Rec |
| schließen, Schließung | close | Close |
| Segment | segment | Segm |
| Signatur | signature | Sig |
| Sprache | language | Lang |
| Standard | standard | Std |
| Status | status | Stat |
| Stornierung | cancellation | Cancel |
| Stückelung | denomination | Denom |
| Synchronisierung | synchronization | Sync |
| Telefon | telephone | Tel |
| terminiert | post-dated | Postdated |
| Transaktion | transaction | Tran* |
| Typ | type | Type |
| Überweisung | remittance | Remitt |
| Unter~ (z.B. Unterkonto) | subsidiary | Sub |
| unterstützt | supported | Supported |
| Verfahren | procedure | Proc |

| | | |
|-----------------|----------------------|--|
| Kapitel: VII | Version: 4.0 | Financial Transaction Services (FinTS) Dokument: XML-Syntax |
| Seite: 148 | Stand: 09.07.2004 | Kapitel: Anhang: Konventionen zur Bildung von Elementnamen Abschnitt: Webservices |

| Deutscher Begriff | Englische Entsprechung | Standard-Kürzel |
|-----------------------|------------------------|-----------------|
| Version | version | Ver |
| Vormerkung | registration | Reg |
| Wert | value | Val |
| Währung | currency | Ccy* |
| wiederkehrend | recurring | Recurr |
| Zahlung | payment | Paymt |
| Zahlungsempfänger | payee | Payee |
| Zeit | time | Time |
| zeitweilig, vorläufig | temporary | Temp |
| Zins | interest | Int |
| Zusatz | extension | Ext |