

Financial Transaction Services (FinTS) Dokument: Security - Sicherheitsverfahren PIN/TAN	Version: 3.0	Kapitel: D
Kapitel: <a href="#">Data-Dictionary</a> Abschnitt: <a href="#">PIN/TAN-Management</a>	Stand: 09.02.2006	Seite: 85

Typ: DE  
Format: an  
Länge: ..99  
Version: 1

### Benutzerdefinierte Signatur

Enthält im Falle des PIN/TAN-Verfahrens die PIN und evtl. eine TAN. Die PIN ist in jeder Nachricht zu senden. Ob eine TAN erforderlich ist, hängt von den im HIPINS-Segment festgelegten Anforderungen der Geschäftsvorfälle ab.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	<a href="#">PIN</a>	DE	an	..99	M	1	
2	<a href="#">TAN</a>	DE	an	..99	O	1	

Typ: DEG  
Format:  
Länge:  
Version: 1

### Bezugssegment

Sofern sich ein Kreditinstitutssegment auf ein bestimmtes Kundensegment bezieht (z.B. Antwortrückmeldung auf einen Kundenauftrag) hat das Kreditinstitut die Segmentnummer des Segments der Kundennachricht einzustellen, auf das sich das aktuelle Segment bezieht (s. DE „Segmentnummer“). In Zusammenhang mit den Angaben zur Bezugsnachricht aus dem Nachrichtenkopf ist hierdurch eine eindeutige Referenz auf das Segment einer Kundennachricht möglich.

Falls die Angabe eines Bezugssegments erforderlich ist, ist dieses bei der Formatbeschreibung eines Kreditinstitutsegments angegeben.

Typ: DE  
Format: num  
Länge: ..3  
Version: 1

### Challenge

Dieses Datenelement enthält im Falle des Zwei-Schritt-TAN-Verfahrens die Challenge zu einem eingereichten Auftrag. Aus der Challenge wird vom Kunden die eigentliche TAN ermittelt. Die Challenge wird unabhängig vom Prozessvariante 1 oder 2 in der Kreditinstitutsantwort im Segment HITAN übermittelt.

- Bei der Challenge kann es sich abhängig vom konkreten
- Zwei-Schritt-Verfahren um eine „Auftragsquersumme“, einen Hashwert, einen Index auf eine bestimmte TAN in einer Liste o. ä. handeln. Bei dynamischen TAN-Generatoren ist es auch möglich, dass die Challenge eine textuelle Anweisung enthält, beispielsweise in der Form „Tippen Sie bitte die ersten sechs Stellen der Auftragge-

Kapitel: D	Version: 3.0	Financial Transaction Services (FinTS) Dokument: Security - Sicherheitsverfahren PIN/TAN
Seite: 86	Stand: 09.02.2006	Kapitel: <a href="#">Data-Dictionary</a> Abschnitt: <a href="#">PIN/TAN-Management</a>

berkontonummer und die letzten beiden Stellen des Betrags in den TAN-Generator ein“. Das Kundenprodukt braucht i. d. R. die Bildungsregel für die Challenge bzw. die Ableitung der TAN aus der Challenge nicht zu kennen – dies ist nur zwischen Kunde und Kreditinstitut vereinbart und Inhalt der Verfahrensanweisung des jeweiligen Instituts.

Typ: DE  
Format: an  
Länge: ..999256  
Version: 1

### Challenge

Dieses Datenelement enthält im Falle des Zwei-Schritt-TAN-Verfahrens die Challenge zu einem eingereichten Auftrag. Aus der Challenge wird vom Kunden die eigentliche TAN ermittelt. Die Challenge wird unabhängig vom Prozessvariante 1 oder 2 in der Kreditinstitutsantwort im Segment HITAN übermittelt.

- Bei der Challenge kann es sich abhängig vom konkreten Zwei-Schritt-Verfahren um eine „Auftragsquersumme“, einen Hashwert, einen Index auf eine bestimmte TAN in einer Liste o. ä. handeln. Bei dynamischen TAN-Generatoren ist es auch möglich, dass die Challenge eine textuelle Anweisung enthält, beispielsweise in der Form „Tippen Sie bitte die ersten sechs Stellen der Auftraggeberkontonummer und die letzten beiden Stellen des Betrags in den TAN-Generator ein“. Das Kundenprodukt braucht i. d. R. die Bildungsregel für die Challenge bzw. die Ableitung der TAN aus der Challenge nicht zu kennen – dies ist nur zwischen Kunde und Kreditinstitut vereinbart und Inhalt der Verfahrensanweisung des jeweiligen Instituts.

Typ: DE  
Format: an  
Länge: ..999  
Version: 2

### **Challenge-Betrag erforderlich**

Über diesen BPD-Parameter erhält die Kundenseite die Information, ob im Rahmen der „[Parameter Challenge-Klasse](#)“ auch der Betrag übermittelt werden soll oder ob dies nicht zugelassen ist.