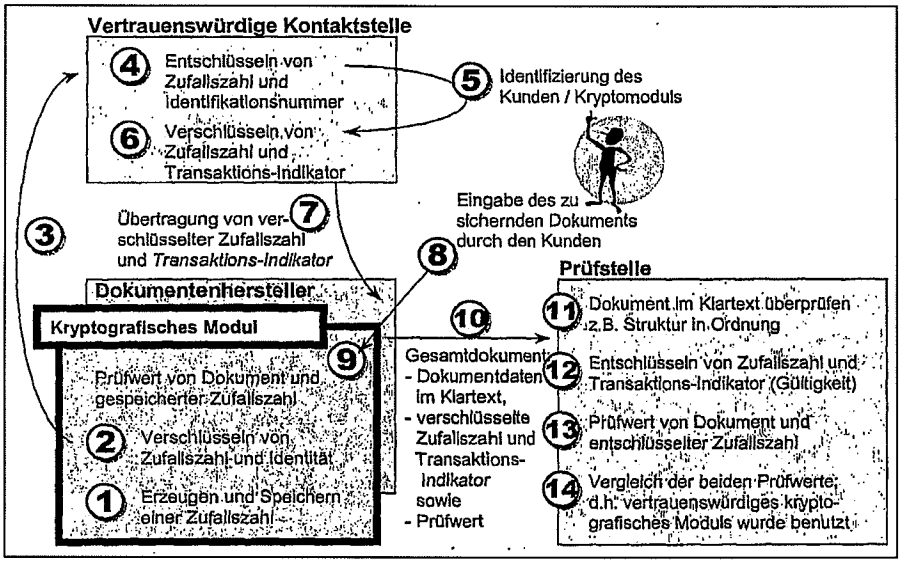
Figure 1



Document producer

Cryptographic module

1 Generating and storing a random number

2 Encrypting the random number and identity

3 ϕ

Reliable contact station

4 Decrypting the random number and the identification number

5 Identifying the customer / crypto-module

6 Encrypting the random number and the transaction indicator

7 Transmitting the encrypted random number and the transaction indicator

8 Entry by the customer of the document to be protected

9 Check value of the document and of the stored random number

10 Entire document:
- document data in plain text
- encrypted random number and transaction indicator as well as
- check value

Checking station

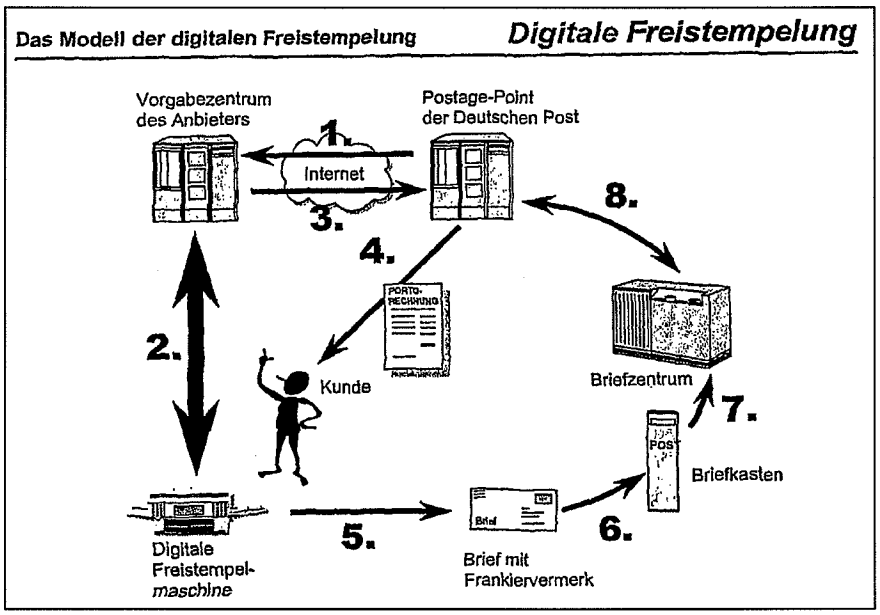
11 Checking document in plain text, e.g. structure correct

12 Decrypting the random number and the transaction indicator (validity)

13 Check value of the document and of the decrypted random number

14 Comparing the two check values; i.e. reliable cryptographic module was used

Figure 2



The model of digital franking ***Digital Franking***

Specification center of the operator

1. ϕ

Internet

3. γ

Postage Point of the Deutsche Post

8. ν

4. Postage invoice

Mail center

κ 7.

2. o

Customer

Mailbox

κ

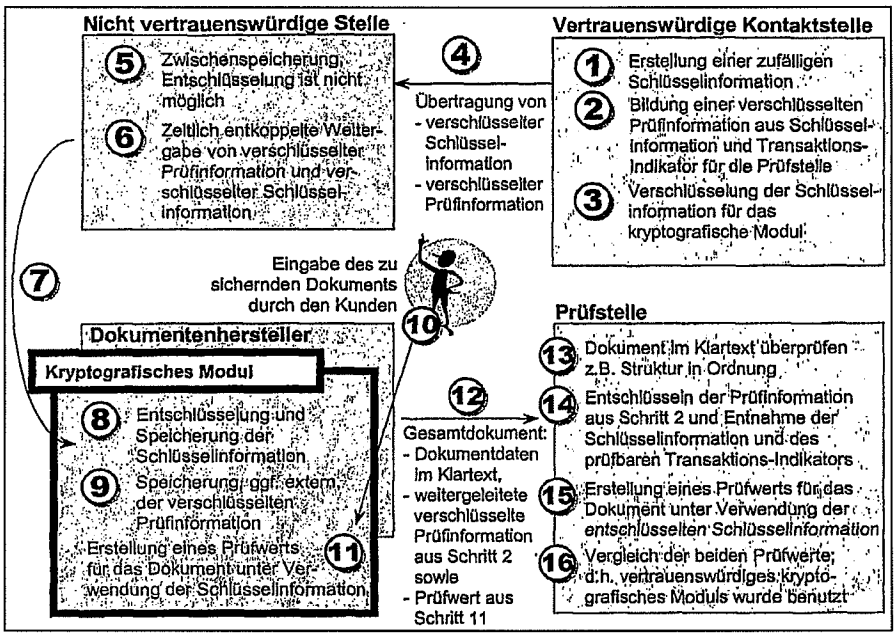
6.

Digital franking machine

5. γ

Letter with postage indicium

Figure 3



Reliable contact station

1 Generating random key information

2 Forming encrypted checking information from key information and from the transaction indicator for the checking station

3 Encrypting the key information for the cryptographic module

4 Transmitting
- encrypted key information
- encrypted checking information

Non-reliable station

5 Intermediate storage, decryption is not possible

6 Forwarding encrypted checking information and encrypted key information at a different point in time

7 ι

Document producer

Cryptographic module

8 Decrypting and storing the key information

9 Storing the encrypted checking information – optionally externally

10 Entry by the customer of the document to be protected

11 Forming a check value for the document using the key information

12 Entire document:
- document data in plain text
- forwarded encrypted checking information from Step 2 as well as
- check value from Step 11

Checking station

13 Checking document in plain text, e.g. structure correct

14 Decrypting the checking information from Step 2 and removing the key information and the checkable transaction indicator

15 Forming a check value for the document using the decrypted key information

16 Comparing the two check values; i.e. a reliable cryptographic module was used