**PCT** WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

**(51) Internationale Patentklassifikation** 6 :
**H04L 1/12**

**A2**

**(11) Internationale Veröffentlichungsnummer:** **WO 98/11689**

**(43) Internationales Veröffentlichungsdatum:** 19. März 1998 (19.03.98)

**(21) Internationales Aktenzeichen:** PCT/EP97/05012

**(22) Internationales Anmeldedatum:** 13. September 1997 (13.09.97)

**(30) Prioritätsdaten:**
196 37 319.0 13. September 1996 (13.09.96) DE

**(71) Anmelder** *(für alle Bestimmungsstaaten ausser US)*: TEMIC TELEFUNKEN MICROELECTRONIC GMBH [DE/DE]; Theresienstrasse 2, D-74072 Heilbronn (DE).

**(72) Erfinder; und**
**(75) Erfinder/Anmelder** *(nur für US)*: BRUHNKE, Michael [DE/DE]; Hiltensperger Strasse 3, D-80792 München (DE). FRIEDRICH, Ferdinand [DE/DE]; Tucherstrasse 26a, D-90562 Heroldsberg (DE).

**(74) Anwalt:** KOLB, Georg; Temic Telefunken microelectronic GmbH, Theresienstrasse 2, D-74072 Heilbronn (DE).

**(81) Bestimmungsstaaten:** AU, BR, JP, KR, MX, NZ, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

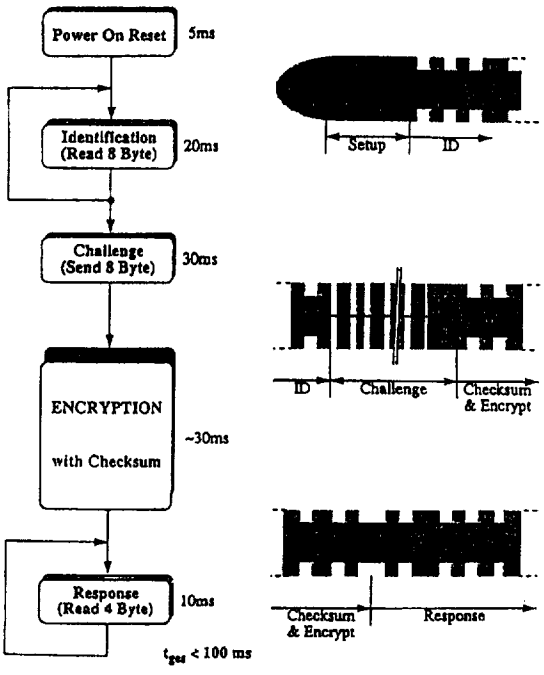
**Veröffentlicht**
*Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.*

**(54) Title:** METHOD OF CRYPTOLOGICAL AUTHENTIFICATION IN A SCANNING IDENTIFICATION SYSTEM

**(54) Bezeichnung:** VERFAHREN ZUR KRYPTOLOGISCHEN AUTHENTIFIZIERUNG IN EINEM RADIOFREQUENZ-IDENTIFIKATIONS-SYSTEM

**(57) Abstract**

The inventive method of cryptological authentification, applied in a scanning identification system with a station base which powers a transponder connected to the object to be identified across the alternating field of an enquiry signal, includes the following steps. For virtually all communications from the base station to the transponder, the base station transmits an enquiry signal. Upon receiving the enquiry signal from the base station, the transponder indicates an identification number stored therein. The base station then encodes a base station generated first bit sequence using a key bit sequence allocated to the transponder identification number and transmits to the transponder the second bit sequence thus obtained. Upon reception of the second bit sequence, the transponder generates from the second bit sequence a supervisory bit sequence which it sends to the base station once it has received the complete second bit sequence. The supervisory bit sequence is intended to check whether the second bit sequence was correctly received. For the purpose of cryptographic authentification, the transponder encodes the first bit sequence reconstructed from the second bit sequence using the key bit sequence allocated to said transponder and transmits to the base station the third bit sequence thus obtained. While the transponder encodes the second bit sequence and converts it to a third bit sequence, the base station verifies using the checking bit sequence, whether a mistake has occured when transferring the second bit sequence, and possibly interrupts the on-going encoding process in the transponder. This may abort the authentification process as no valid result can be reckoned with and allows for time to be saved for relaunching the whole authentification process.



**(57) Zusammenfassung**

Das Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System mit einer Basisstation, die einen mit dem zu identifizierenden Objekt verbundenen Transponder über das Wechselfeld eines Abfragesignals mit Energie versorgt, weist folgende Verfahrensschritte auf. Für die im wesentlichen gesamten Kommunikationen zwischen Basisstation und Transponder erzeugt die Basisstation ein Abfragesignal. Der Transponder antwortet bei Empfang des von der Basisstation gesendeten Abfragesignals mit einer in seinem Speicher abgelegten Identifikationsnummer. Daraufhin verschlüsselt die Basisstation eine von ihr generierte erste Bitfolge anhand einer Schlüsselbitfolge, die der Identifikationsnummer des Transponders zugeordnet ist und sendet die so erhaltene zweite Bitfolge zum Transponder. Beim Empfang der zweiten Bitfolge generiert der Transponder aus der zweiten Bitfolge eine Kontrollbitfolge und sendet diese nach vollständigem Empfang der zweiten Bitfolge an die Basisstation. Diese Kontrollbitfolge dient zur Überprüfung des richtigen Empfangs der zweiten Bitfolge. Zur Kryptographischen Authentifizierung verschlüsselt der Transponder die aus der zweiten Bitfolge rekonstruierte erste Bitfolge anhand der dem Transponder zugeordneten Schlüsselbitfolge und sendet die so erhaltene dritte Bitfolge zur Basisstation. Noch während der Transponder die zweite Bitfolge zur dritten Bitfolge verschlüsselt, überprüft die Basisstation anhand der Kontrollbitfolge, ob bei der Übertragung der zweiten Bitfolge ein Fehler aufgetreten ist, unterbricht gegebenenfalls die laufende Verschlüsselung im Transponder. Dadurch kann die laufende Authentifizierung unterbrochen werden, da nicht mit einem richtigen Ergebnis gerechnet werden kann. Es wird Zeit beim Start eines erneuten Durchlaufs des Authentifizierungsverfahrens gewonnen.

Beschreibung

# Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System

Die Erfindung betrifft Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System.

Bei der Identifikation von Personen, Tieren und Objekten hat sich in den letzten Jahren ein System bewährt, bei dem ein (stationäres bzw. tragbares) Lesegerät, auch Reader oder Basisstation genannt, einen mit dem zu identifizierenden Objekt verbundenen Transponder über ein Wechselfeld mit Energie versorgt, woraufhin der Transponder mit dem Aussenden der in ihm gespeicherten Daten antwortet. Aufgrund des verwendeten Frequenzbereichs spricht man auch von Radiofrequenz-Identifikations-Systemen, kurz RFID.

Ein RFID-Transponder besteht im allgemeinen aus einer Antennenspule und einem integrierten Schaltkreis, der alle notwendigen elektronischen Schaltungsblöcke, wie z. B. zur Spannungsversorgung, zur Taktgenerierung, zur Ablaufsteuerung und zur Speicherung der für die Identifizierung notwendigen Daten, beinhaltet. Die zur Antennenspule parallelgeschaltete Kapazität ist ebenfalls häufig Bestandteil des integrierten Schaltkreises. Sie kann jedoch auch durch ein diskretes Bauelement gebildet werden.

Das RFID-Lesegerät besteht aus einem Schwingkreis mit einer Sendespule und einer Kapazität, der von einer Treiberstufe mit einem Signal mit einer im allgemeinen festen Frequenz (z. B. 125 kHz) angesteuert wird. Weiterhin enthält das Lesegerät elektronische Schaltungsblöcke, um die durch die Absorptionsmodulation vom Transponder gesendeten Daten zu erkennen

und um Daten und Befehle, z. B. durch Modulation des Feldes, an den Transponder zu senden.

Lesegerät und Transponder bilden bei der Daten- bzw. bei der Energieübertragung einen lose gekoppelten Transformator. Deshalb ist die Energieübertragung relativ gering.

Die erzielbare Reichweite für die kontaktlose Übertragung von Energie und Daten wird durch folgende Randbedingungen beeinflußt:

- Sendeenergie (beschränkt durch gesetzliche Bestimmungen)
- Spulenabmessungen
- Störpegel der Umgebung
- Übereinstimmung der Resonanzfrequenzen
- Modulationshub
- Spannungsverlust über den Gleichrichter
- Verwendete Übertragungsverfahren

Beispielsweise in der Anwendung in Form einer Wegfahrsperre ergeben sich durch die kleine um das Zündschloß herum angeordnete Sendespule extrem ungünstige Übertragungsbedingungen. Darum gilt es, das System auf minimale Verluste hin zu optimieren. Entscheidend ist dabei:

- Gleiche Resonanzfrequenz von Basisstation und Transponder
- Zeitlich optimierte Übertragungsprotokolle
- Minimale Verluste bei der Energieübertragung
- Maximaler Modulationshub bei der Datenübertragung zur Basisstation (Read)
- Optimierte Datenübertragung zum Transponder (Send)

Beim Starten eines Kfz nimmt der Anwender eine Zeitdauer von mehr als 150 ms, vom Drehen des Zündschlüssels bis zum Starten des Motors, als Zeitverzögerung war. Daraus folgt, daß das gesamte Übertragungsprotokoll in diesem sehr kurzen Zeitraum abgelaufen sein muß. Dabei gilt es mehrere Punkte zu beachten. Zum einen sollte eine einmalige Datenübertragung das korrekte Ergebnis liefern, zum anderen sollten zusätzliche Funktionen wie

die Authentifizierung mittels eines Algorithmus in einer möglichst kurzen Zeit ablaufen.

Aufgabe der Erfindung ist es, ein Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System anzugeben, das in einer möglichst kurzen Zeit abläuft.

Diese Aufgabe wird durch ein Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System mit den Merkmalen der Ansprüche 1 und 4 gelöst. Die Vorteilhafte Ausgestaltung der Erfindung erfolgt geäß den Merkmalen der abhängigen Ansprüche.

Das Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System mit einer Basisstation, die einen mit dem zu identifizierenden Objekt verbundenen Transponder über das Wechselfeld eines Abfragesignals mit Energie versorgt, weist folgenden Verfahrensschritte auf.

Für die im wesentlichen gesamte Kommunikation zwischen Basisstation und Transponder erzeugt die Basisstation ein Abfragesignal. Der Transponder antwortet bei Empfang des von der Basisstation gesendeten Abfragesignals mit einer in seinem Speicher abgelegten Identifikationsnummer. Daraufhin verschlüsselt die Basisstation eine von ihr generierte erste Bitfolge anhand einer Schlüsselbitfolge, die der Identifikationsnummer des Transponders zugeordnet ist und sendet die so erhaltene zweite Bitfolge zum Transponder.

Beim Empfang der zweiten Bitfolge generiert der Transponder aus der zweiten Bitfolge eine Kontrollbitfolge und sendet diese nach vollständigen Empfang der zweiten Bitfolge an die Basisstation. Diese Kontrollbitfolge dient zur Überprüfung des richtigen Empfangs der zweiten Bitfolge. Zur Kryptographischen Authentifizierung verschlüsselt der Transponder die aus der zweiten Bitfolge rekonstruierte erste Bitfolge anhand der dem Transponder zugeordneten Schlüsselbitfolge und sendet die so erhaltene dritte Bitfolge zur Basisstation.

Noch während der Transponder die zweite Bitfolge zur dritten Bitfolge verschlüsselt überprüft die Basisstation anhand der Kontrollbitfolge ob bei der Übertragung der zweiten Bitfolge ein Fehler aufgetreten ist, unterbricht gegebenenfalls die laufende Verschlüsselung im Transponder. Dadurch kann die laufende Authentifizierung unterbrochen werden, da nicht mit einem richtigen Ergebnis gerechnet werden kann. Es wird Zeit beim Start eines erneuten Durchlaufs des Authentifizierungsverfahren gewonnen.

Im anderen Fall prüft die Basisstation die Gültigkeit der empfangenen dritten Bitfolge.

Eine weitere Verkürzung der Zeitdauer für die Authentifizierung wird dadurch erreicht, daß der Transponder die Länge der dritten Bitfolge vor dem Senden an die Basisstation halbiert.

In einer Ausgestaltung des Verfahrens verschlüsselt die Basisstation zu Beginn des Verfahrens sofort eine von ihr generierte ersten Bitfolge anhand einer ihr und dem Transponder zugeordneten Schlüsselbitfolge und sendet die so erhaltene zweite Bitfolge sofort zum Transponderder anstatt erst den Empfang der Identifikationsnummer des Transponder abzuwarten. Dadurch wird eine weitere Verkürzung der Zeitdauer für die Authentifizierung erzielt.

Kurze Beschreibung der Figuren:

Figur 1 zeigt ein Ablaufdiagramm des Verfahrens zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System auf der Transponderseite;

Figur 2 zeigt den Ablauf des Verfahrens in einer Wegfahrsperre für ein Kraftfahrzeug;

Figur 3 zeigt verschiedene Signalverläufe bei der Kommunikation zwischen Basisstation und Transponder;

Figur 4 zeigt ein detailiertes Ablaufdiagramm eines RFID Systems mit Kryptologischer Authentifizierung.

In folgenden wird das Verfahren gemäß der Erfindung unter Zuhilfenahme der Figuren anhand eines Ausführungsbeispiels erläutert. Zur näheren Erläuterung des Prinzips einer kryptologischen Authentifizierung wird auf das von TEMIC speziell für hohe Sicherheitsanforderungen, wie z. B. der Wegfahrsperre entwickelte und optimierte Verfahren TIME (TEMIC Immobilizer Encryption) eingegangen, das sich durch folgende Merkmale auszeichnet:

- Sichere und schnelle Authentifizierung (< 100 ms)
- Anwendungsoptimierter Hochsicherheitsalgorithmus
- Kundenspezifische Generierung von einzigartigen Schlüsseln

Dadurch wird ein hohes Maß an Sicherheit, sowohl bei der Datenübertragung als auch bei der eigentlichen Verschlüsselung im Zusammenhang mit einer extrem kurzen Authentifizierungszeit erreicht. Figur 1 zeigt den von TEMIC auf minimale Zeitdauer hin optimierten Authentifizierungsablauf. Das besondere ist, erstens die für die Berechnung des Algorithmus benötigte geringe Zeitdauer (Encryption time 30 ms), zweitens die Verkürzung der Response von acht auf vier Byte durch ein besonderes Verfahren und drittens die Möglichkeit den Ablauf beim Erkennen eines Fehlerfalles jederzeit unterbrechen zu können.

Bei der Initialisierung des RFID Systems wird dem Transponder und der Basisstation ein gemeinsamer, die Funktion des Krypto-Algorithmus bestimmender und speziell generierter, 120 Bit langer kryptologischer Schlüssel, der sogenannte Crypto Key, übergeben. Dieser Schlüssel ist im Gesamtsystem einzigartig. Kein anderes RFID System, d.h. keine weitere Basisstation und kein weiterer Transponder besitzt diesen Schlüssel.

Im Betrieb sendet der Transponder nach der Synchronisation (Setup) mit der Basisstation eine eindeutig bestimmte Bitfolge (String) fester Länge (abhängig von der Applikation, z. B. 64 Bit), den sogenannten ID-Code oder kurz ID, an die Basisstation. Diese ID wird in der Regel zur Schlüsselidentifikation verwendet. Dieses ist erforderlich, wenn

unterschiedliche Transponder (mit unterschiedlichen Krypto-Schlüsseln) mit einer Basisstation zusammenarbeiten sollen.

Bei dem verwendeten Authentifizierungsprotokoll handelt es sich um ein Challenge- und Response-Protokoll, wie es in der Figur 2 dargestellt ist, mit dem Merkmal, daß „Known Plaintext"- und „Choosen Plaintext"-Attacken erfolglos sind.

Die Basisstation generiert eine 64 Bit-Zufallszahl Z und verschlüsselt diese mittels eines 32 Bit-Teilschlüssels, der aus dem Crypto-Key generiert wird. Das erhaltene 64 Bit-Zufallsergebnis - die sogenannte Challenge - wird an den Transponder gesendet. Lediglich ein Transponder, der denselben Teilschlüssel besitzt, ist in der Lage, den Zufallswert zu rekonstruieren. Ein Beobachter des Protokolls ist somit nicht in der Lage die Zufallszahl Z herauszubekommen. Der Transponder und die Basisstation verschlüsseln die Challenge mittels des 120 Bit-Crypto-Keys, unter Verwendung eines speziell entwickelten Algorithmus AUT 64. Aus dem 64 Bit-Verschlüsselungsergebnis wird jeweils eine 32 Bit-Zeichenfolge generiert. Der Transponder sendet diese Zeichenfolge - die sogenannte Response - an die Basisstation. Bei Übereinstimmung der gesendeten Response und des generierten Strings akzeptiert die Basisstation die Authentizität des Transponders.

Der verwendete Algorithmus AUT 64 ist eine byte-orientierte Blockchiffre, die aus 64 Bit unter Verwendung eines 120 bit Crypto Keys Output-Strings generiert. Ein 64 Bit-Inputstring (hier die Zufallszahl Z) wird durch Verschlüsselung - in 24 Runden - in einen 64 Bit-Outputstring (hier das Verschlüsselungsergebnis) überführt. In jeder Runde wird ein anderer aus dem Crypto-Key generierter Schlüssel verwendet. Durch diese Vorgehensweise wird das hohe Maß an Sicherheit erreicht. Statistische Analysen bestätigen das auf eindruckvolle Weise. Begründet ist dieses im wesentlichen durch eine nichtlineare Verschlüsselung, die in jeder Runde unterschiedlich (schlüsselgesteuert) gewählt wird.

Key-Erzeugung: Für die Generierung des 120 Bit-Crypto-Keys stellt TEMIC ein Programm zur Verfügung, das unter anderem den Data-Encryption-Standard (DES) als Zufallsgenerator verwendet. Damit wird gewährleistet, daß lediglich der Anwender das Wissen über den Crypto-Key hat.

Der für den AUT 64 benutzte 120 Bit-Crypto-Key besteht aus den Komponenten Family-Key (24 Bit), User-Key (64 Bit) und Random-Key (32 Bit). Der User-Key wird vom Hersteller mittels eines Serial-Keys generiert.

Random-Key: Der Random-Key wird mittels des DES erzeugt. Der zugehörige 56 Bit-DES-Schlüssel sowie den DES-Input bestimmt der Benutzer, so daß TEMIC keine Information über den DES-Output und somit über den generierten Random-Key besitzt.

Family-Key: Die jeweiligen Schlüssel werden mittels eines speziellen Programms erzeugt, wobei insbesondere garantiert wird, daß unterschiedliche Benutzer verschiedene Gruppen von Family-Keys der Länge 24 Bit erhalten. Jedem Benutzer werden dabei 12 Bit so zugeordnet, daß er aus einem Bereich von 16 Zahlen wählen kann. Dieses ist das einzige Wissen, das TEMIC über die später zum Einsatz kommenden Schlüssel besitzt.

User-Key: Mittels eines speziellen Verfahrens wird dabei eine einmalige 64 Bit-Zufallszahl erzeugt, d. h., daß jeder User-Key nur einmal erzeugt wird. Eine Wiederholung findet erst nach $20{,}9 * 10^{12}$ erzeugten User-Keys statt.

Verkürzung des Übertragungsprotokolls durch:

- Es muß nicht erst das Senden des gesamten ID-Codes (Identifikation) abgewartet werden, sondern die Challenge könnte bereits nach dem Power-on-Reset gesendet werden -> einsparen von 20 ms.
- Während der Berechnung des Algorithmus (Encryption, Verschlüsselung der Challenge) wird eine Checksumme zur Basisstation gesendet. Damit wird geprüft, ob die Challenge korrekt übertragen wurde. Sollte diese nicht korrekt sein, so kann die Encryption sofort durch Senden eines Gap unterbrochen werden und eine neue Challenge gesendet werden. Es muß also nicht erst die zwangsläufig falsche und somit nutzlose Response abgewartet werden.
- Das Ergebnis der Encryption besteht wie der Input (die Challenge) aus 8 Byte. Diese 64 Bit werden beispielsweise durch eine XOR-Funktion verknüpft, so daß lediglich 4 Byte als Ergebnis (Response) zur Basisstation zurückübertragen werden brauchen. -> Halbierung der Zeit (bei diesem Beispiel von 20 ms auf 10 ms).

Hochsicherheitsalgorithmus:

- Die Zufallszahl, d. h. der Input für den AUT 64-Algorithmus wird nicht direkt übertragen, sondern zunächst verschlüsselt (Ergebnis = die Challenge) -> keine choosen plaintext attacks möglich.
- Der Algorithmus AUT 64 wird 24 mal durchlaufen und dabei in jeder Runde variiert, d. h. die nichtlineare Verschlüsselung wird in jeder Runde unterschiedlich (schlüsselgesteuert) gewählt. -> Algorithmus schwer „zu brechen".

Key-Erzeugung:

- Ein Teilschlüssel - der User-Key - wird mittels eines speziellen Verfahrens so erzeugt, daß er einmalig ist. Eine Wiederholung findet erst nach $20{,}9 * 10^{12}$ erzeugten User-Keys statt.
- Nur der Anwender hat Einfluß auf die Generierung des Random-Keys - weder TEMIC noch andere haben darüber Information.
- Beim Family-Key vergibt TEMIC einen Teilbereich an jeden Anwender. Dieser Anwender, z. B. ein Kfz-Hersteller, kann aus einem Bereich von 16 Zahlen wählen und somit jeder Kfz-Serie (z. B. jedem VW Golf) einen bestimmten Family-Key-Teilschlüssel zuordnen. -> Jeder Anwender bekommt einen bestimmten Teilschlüsselbereich, womit sich auch der auf die Schlüssel zugreifende Algorithmus unterscheidet (z. B. VW und Opel haben verschiedene Schlüssel).

Die Datenübertragung bei dem hier beschriebenen Verfahren kann in drei Bereiche unterteilt werden:

- Read-Mode = Datenübertragung vom Transponder zu der Basisstation
- Send-Mode = Datenübertragung von der Basisstation zum Transponder
- Write-Mode = Datenübertragung von der Basisstation zum Transponder mit anschließender Programmierung

Um die Datenintegrität, d. h., die manipulationsfreie und somit unveränderte Datenübertragung bei den einzelnen Modes zu gewährleisten, kommen verschiedene Möglichkeiten zur Anwendung.

Im Read-Mode werden Daten (ID-Code) aus dem EEPROM-Speicher des Transponders ausgelesen und zu der Basisstation gesendet. Die ersten 8 Bit stellen dabei einen kundenspezifischen Header dar, der von TEMIC programmiert und gegen Manipulation gesichert wird. Die anderen Bits sind vom Kunden frei programmierbar und beinhalten normalerweise eine fortlaufende Nummer samt Checksumme, so daß eine fehlerhafte Übertragung des Codes erkannt werden kann.

Vorteil: Header und Checksumme werden geprüft.

Der Send-Mode wird bei der Übertragung des Startwertes (Challenge) für die Authentifizierung verwendet. Der Transponder überprüft dabei die korrekte Anzahl der übertragenen Bits sowie der Feldtakte zwischen den Feldlücken. Anschließend sendet er eine aus der Anzahl der übertragenen „Einsen" gebildete Checksumme zur Verifikation der korrekten Übertragung an die Basisstation (Bild 5). Sollte die Checksumme nicht korrekt sein, so besteht die Möglichkeit den Authentifizierungsprozeß zu unterbrechen und erneut zu starten.

Vorteil: Bitanzahl und Taktanzahl zwischen den Feldlücken sowie Senden der Checksumme werden geprüft.

Das TEMIC-Schreibverfahren basiert auf der ON/OFF-Tastung des vom Lesegerätes erzeugten RF-Feldes. Die Information ist in der Anzahl der Feldtakte zwischen zwei Feldlücken enthalten (Figur3). Durch Dekodierung des zwischen zwei Pausen erreichten Zählerstandes werden die gesendeten Bits erkannt. Es ist auch möglich, zusätzlich zu der Dateninformation Steuersignale zu übertragen. Dazu werden weitere Zählerstände definiert. Der Übergang vom Lesebetrieb in den Sendebetrieb wird durch eine Feldlücke eingeleitet, woraufhin die Chipkarte auf „Send-Mode" umschaltet und die nachfolgenden Daten aufnimmt. Die Datenübertragung wird auf Gültigkeit und Anzahl der Datenbits überprüft. Der Send-Mode wird verlassen, wenn nicht nach spätestens 64 Feldtakten eine Pause erkannt wird.

Beim Write-Mode werden die Daten zunächst von der Basisstation zu dem Transponder übertragen und anschließend in das EEPROM programmiert.

Wie im Send-Mode wird auch hierbei die korrekte Übertragung der Datenbits geprüft. Ist der zu beschreibende Speicherbereich gegen Manipulation gesichert, indem das entsprechende Lockbit gesetzt ist, so wird dieses vom IDIC registriert und eine Programmierung verhindert (Figur 4). Sollten alle beschriebenen logischen Überprüfungen positiv ausfallen, so wird die zum Programmieren benötigte hohe Programmierspannung von ca. 16 V intern erzeugt und analog gemessen. Diese Überprüfung findet auch während des gesamten Programmiervorgangs statt. Im Fehlerfall bricht der IDIC die Programmierung sofort ab und geht in den Read-Mode, wobei er den ID-Code überträgt. Dieses besondere Verhalten wird von der Basisstation registriert. Bei einem korrekten Ablauf wird der soeben programmierte Block zur Verifikation an die Basisstation zurückübertragen.

Vorteil: Überprüfungen bevor eine Programmierung erfolgt.

- Übertragung der Daten muß korrekt sein, d. h. übertragene Bitanzahl und Takte zwischen den Feldlücken müssen stimmen.
- Password-Schutz darf nicht gesetzt sein.
- Lockbit darf nicht gesetzt sein.
- HV-Spannung muß groß genug sein (zum Programmieren der EEPROMs werden etwa 16 V benötigt). Dieses wird vor und wähend des Programmierens geprüft.

Im Fehlerfall geht der IC sofort, d. h., frühzeitiger in den Read-Mode und sendet Daten. Dieses kann von der Basisstation erkannt werden.

Zum Schutz der gespeicherten Daten sind mehrere Mechanismen implementiert:

- Lockfunktion
- Password-Schutz
- UV-Schutz

Verschiedene Speicherbereiche können durch Setzen von Lockbits separat gegen Manipulation geschützt werden. Diese Lockfunktion kann nicht rückgängig gemacht werden.

Wird der Password-Schutz aktiviert, so können bestimmte Daten lediglich nach dem Senden des korrekten Passwords in den Speicher programmiert bzw. aus dem Speicher gelesen werden. Beispielsweise wird ein nur dem jeweiligen Kunden bekanntes Password vor dem Ausliefern der Transponder programmiert, so daß ein nichtautorisierter Benutzer keinen Zugriff auf den Speicher hat.

Sollte ein Angreifer versuchen, den Password-Schutz oder die Lockfunktion durch Löschen des EEPROMs, z. B. durch UV-Bestrahlung, zu umgehen, so tritt der UV-Schutz in Kraft. Dieser verhindert das Reprogrammieren eines einmal vollständig gelöschten Speichers.

Patentansprüche

1. Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System mit einer Basisstation und einem Transponder, wobei die Basisstation eine erste Bitfolge generiert und an den Transponder sendet, der Transponder aus der ersten Bitfolge mittels eines Kryptographischen Schlüssels eine zweite Bitfolge generiert und diese als Antwort zur Basis zurücksendet, woraufhin die Basis aufgrund dieser Antwort die Nutzungsberechtigung überprüft, dadurch gekennzeichnet, daß der Transponder sofort nach Erhalt der ersten Bitfolge eine Antwort generiert, aus der die Basisstation erkennt, ob bei der Übertragung der ersten Bitfolge ein Fehler aufgetreten ist.

2. Verfahren zum Überprüfen einer Nutzungsberechtigung nach Anspruch 1, dadurch gekennzeichnet, daß die Basisstation den laufenden Vorgang des Generierens der zweiten Bitfolge durch den Transponder abbricht, wenn bei der Übertragung der ersten Bitfolge ein Fehler aufgetreten ist.

3. Verfahren zum Überprüfen einer Nutzungsberechtigung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Länge der zweiten Bitfolge die Hälfte der Länge der ersten Bitfolge beträgt.

4. Verfahren zur kryptologischen Authentifizierung in einem Radiofrequenz-Identifikations-System mit einer Basisstation, die einen mit dem zu identifizierenden Objekt verbundenen Transponder über das Wechselfeld eines Abfragesignals mit Energie versorgt, mit folgenden Verfahrensschritten:

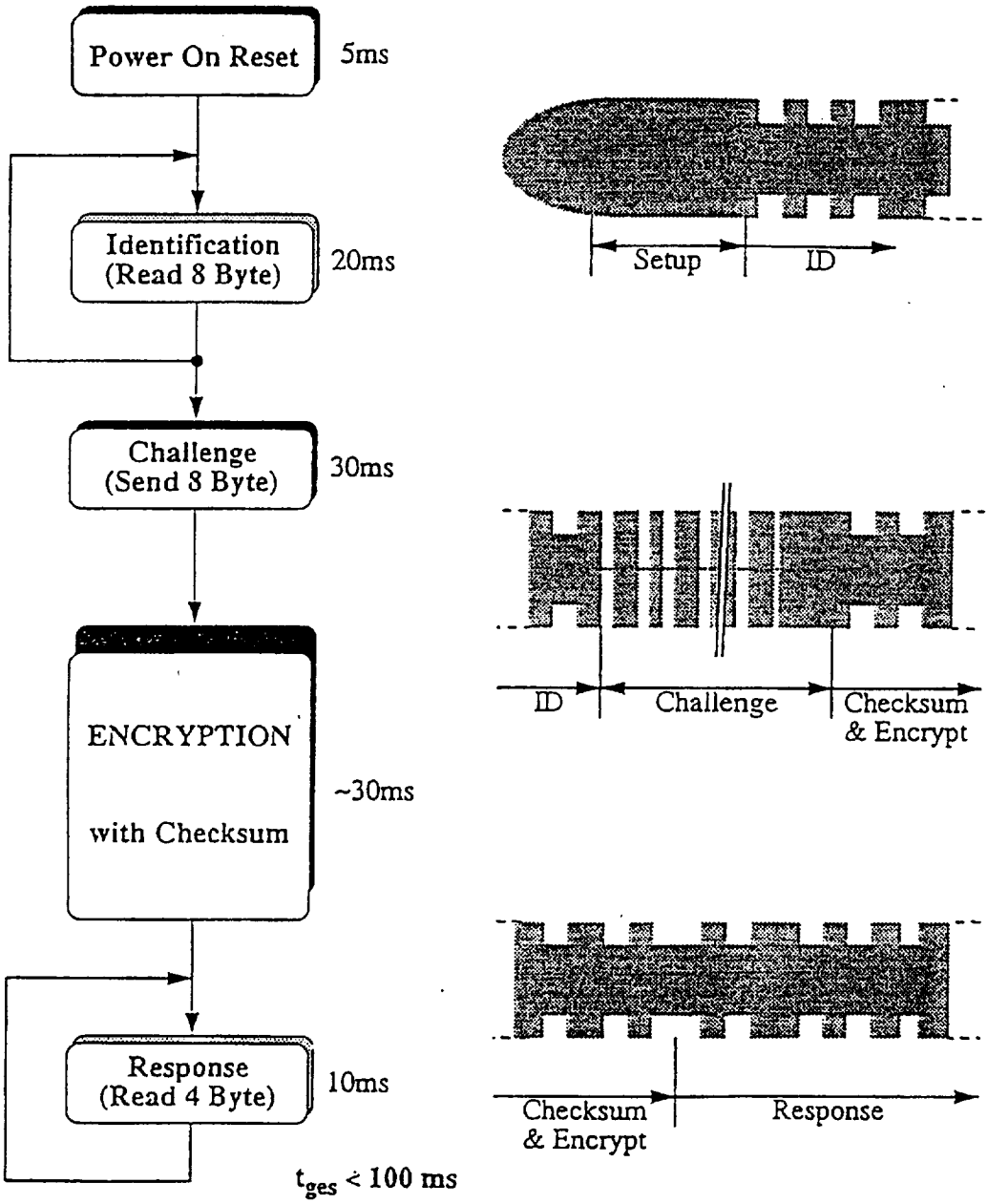
- die Basisstation erzeugt ein Abfragesignal;
- der Transponder antwortet bei Empfang des von der Basisstation gesendeten Abfragesignals mit einer in seinem Speicher abgelegten Identifikationsnummer;
- die Basisstation verschlüsselt eine von ihr generierte ersten Bitfolge anhand einer der Identifikationsnummer des Transponders

zugeordneten Schlüsselbitfolge und sendet die so erhaltene zweite Bitfolge zum Transponder;

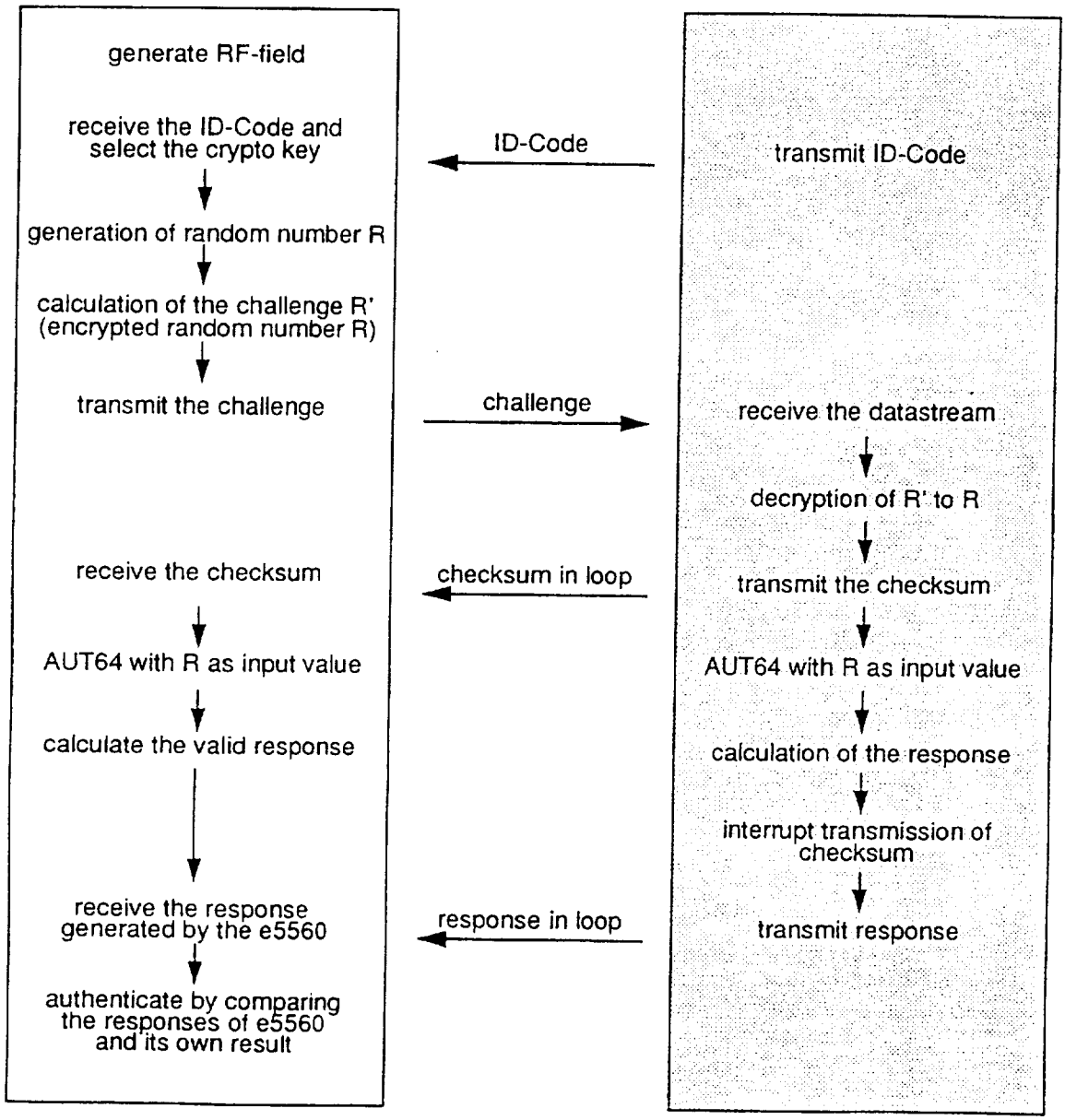
- beim Empfang der zweiten Bitfolge generiert der Transponder aus der zweiten Bitfolge eine Kontrollbitfolge und sendet diese nach vollständigen Empfang der zweiten Bitfolge an die Basisstation
- der Transponder rekonstruiert aus der zweiten Bitfolge die erste Bitfolge und verschlüsselt diese anhand der dem Transponders zugeordneten Schlüsselbitfolge und sendet die so erhaltene dritte Bitfolge zur Basisstation;
- noch während der Transponder die zweite Bitfolge zur dritten Bitfolge verschlüsselt überprüft die Basisstation anhand der Kontrollbitfolge ob bei der Übertragung der zweiten Bitfolge ein Fehler aufgetreten ist, unterbricht gegebenenfalls die laufende Verschlüsselung im Transponder
- die Basisstation prüft die Gültigkeit der empfangenen dritten Bitfolge.

5. Verfahren zur kryptologischen Authentifizierung nach Anspruch 4, dadurch gekennzeichnet, daß der Transponder die Länge der dritten Bitfolge vor dem Senden an die Basisstation halbiert.

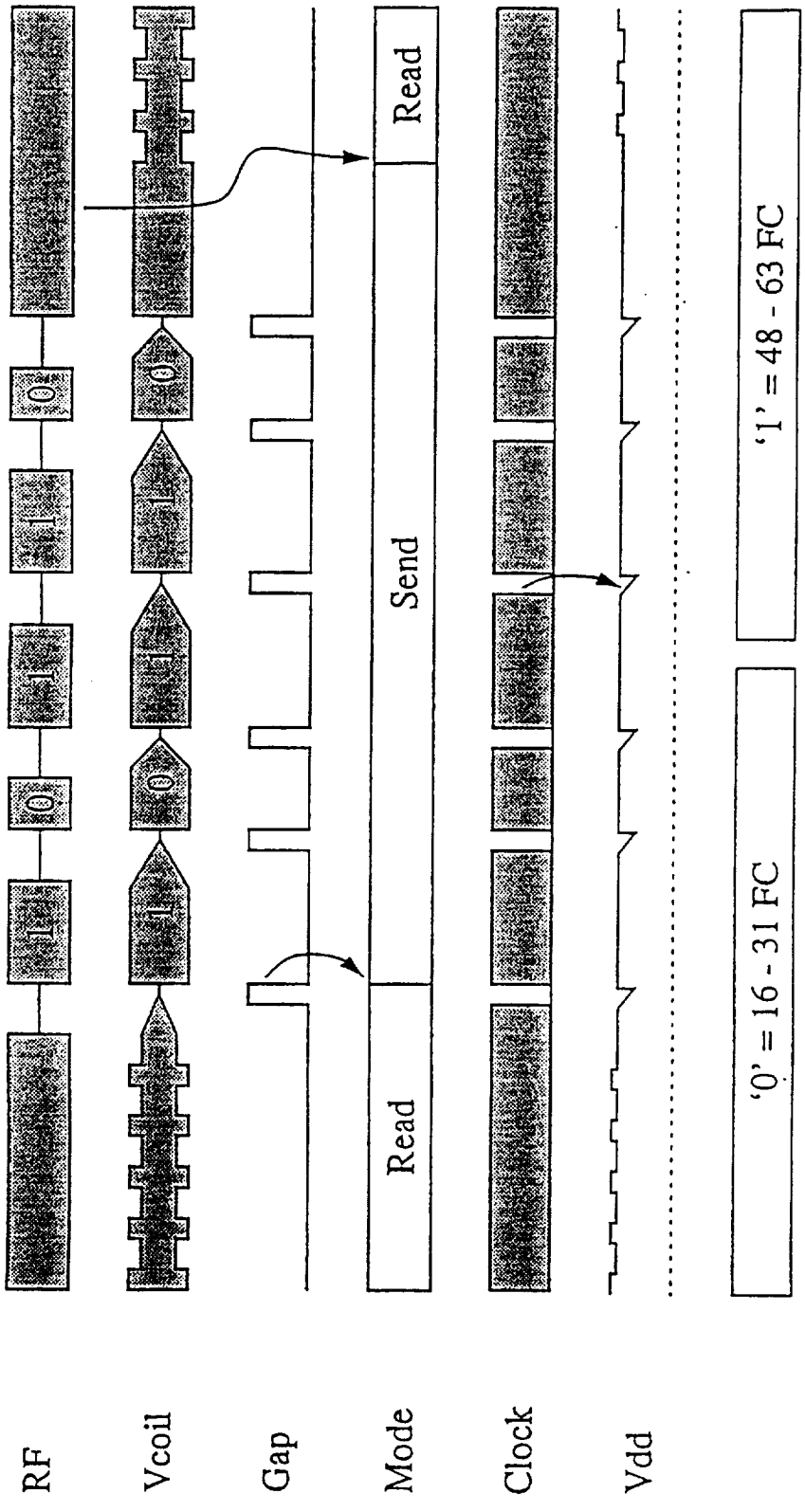
6. Verfahren zur kryptologischen Authentifizierung nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß die Basisstation zu Beginn des Verfahrens sofort eine von ihr generierte ersten Bitfolge anhand einer Ihr und dem Transponder zugeordneten Schlüsselbitfolge verschlüsselt und die so erhaltene zweite Bitfolge zum Transponderder sendet anstatt den Empfang der Identifikationsnummer des Transponder abzuwarten.


Power On Reset
5ms
Identification
(Read 8 Byte)
20ms
Challenge
(Send 8 Byte)
30ms
ENCRYPTION
with Checksum
~30ms
Response
(Read 4 Byte)
10ms
$t_{ges}$ < 100 ms
Setup
ID
ID
Challenge
Checksum
& Encrypt
Checksum
& Encrypt
Response

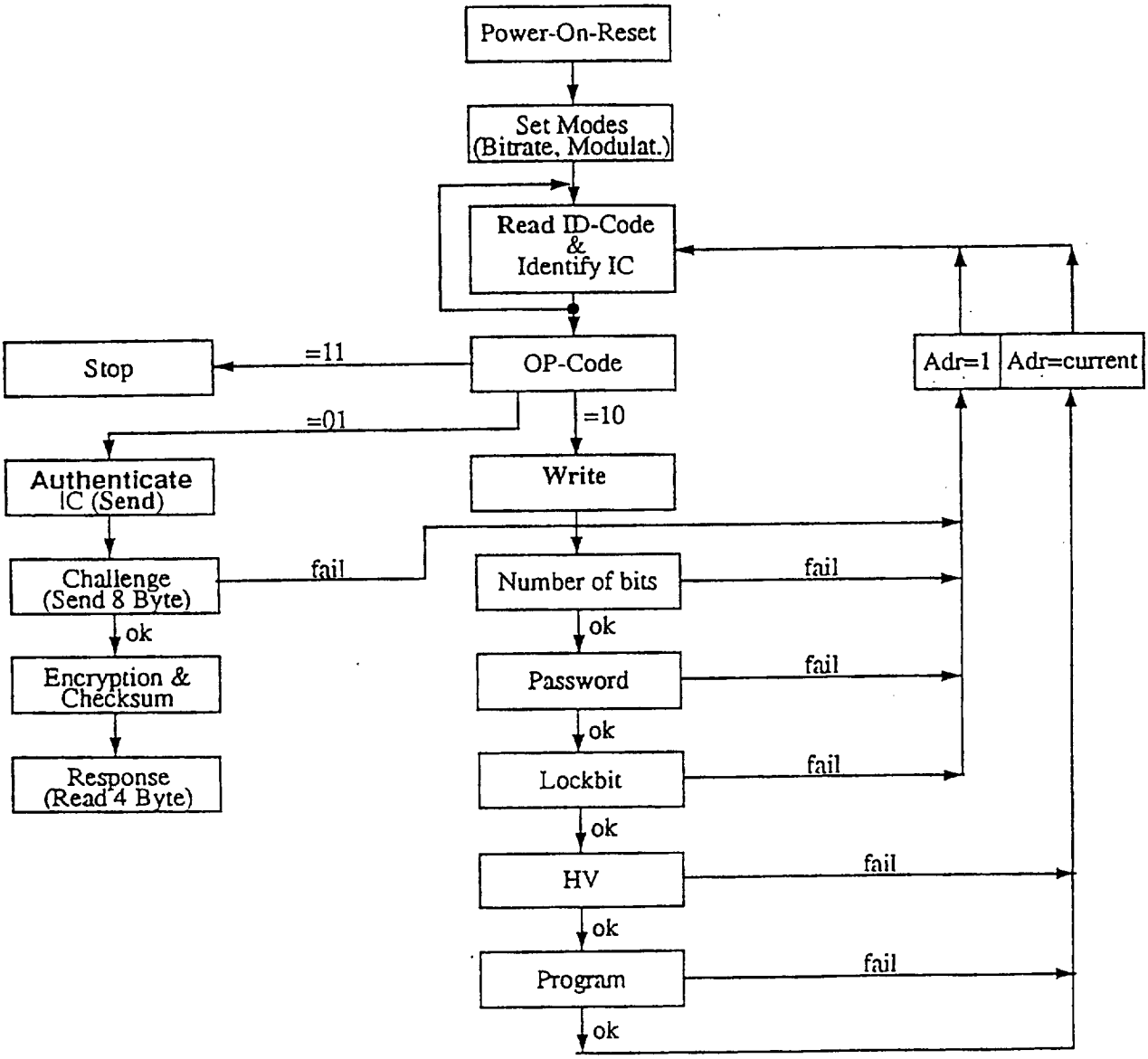
Figur 1


generate RF-field
receive the ID-Code and select the crypto key
generation of random number R
calculation of the challenge R' (encrypted random number R)
transmit the challenge
receive the checksum
AUT64 with R as input value
calculate the valid response
receive the response generated by the e5560
authenticate by comparing the responses of e5560 and its own result
ID-Code
challenge
checksum in loop
response in loop
transmit ID-Code
receive the datastream
decryption of R' to R
transmit the checksum
AUT64 with R as input value
calculation of the response
interrupt transmission of checksum
transmit response

Figur 2




Figur 3


Power-On-Reset
Set Modes (Bitrate, Modulat.)
Read ID-Code & Identify IC
OP-Code
=11
Stop
=01
=10
Authenticate IC (Send)
Challenge (Send 8 Byte)
fail
ok
Encryption & Checksum
Response (Read 4 Byte)
Write
Number of bits
fail
ok
Password
fail
ok
Lockbit
fail
ok
HV
fail
ok
Program
fail
ok
Adr=1
Adr=current

Figur 4