(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 246 135 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
02.10.2002 Patentblatt 2002/40

(51) Int Cl.[7]: **G07B 17/04**

(21) Anmeldenummer: **02090093.2**

(22) Anmeldetag: **01.03.2002**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **29.03.2001 DE 10116703**

(71) Anmelder: **Francotyp-Postalia AG & Co. KG**
16547 Birkenwerder (DE)

(72) Erfinder: **Pauschinger, Dieter, Dr.**
13465 Berlin (DE)

(54) Verfahren zur Aufzeichnung eines Verbrauchswertes und Verbrauchszähler mit einem Messwert

(57) Ein Verbrauchszähler (1) mit Meßwertgeber (104,105), Anzeigeeinheit (4) mit Sicherheitsmitteln (S1, S2, 18), mit einer Zuführ- und Abgabeeinrichtung (8, 6) und eine Kommunikationseinrichtung (101) wird von einem Sicherheitsgehäuse (10) umschlossen. Der Sicherheitsmodul (100) hat einen nichtflüchtigen Speicher (124, 129) zur Speicherung temporär gültiger Tarife und ist programmiert, eine Abgabegebühr basierend auf dem Verbrauchswert tarifabhängig zu berechnen. Ein Verfahren zur Aufzeichnung eines Verbrauchswertes umfaßt eine nichtflüchtige Speicherung von Tarifwerten, Liefern und Verarbeitung von Meßwerten über die Zufuhr und Abgabe von Materie, Energie oder Information, Liefern und Auswerten von Zeitdaten zur Ermittlung mindestens eines Verbrauchswertes, eine tarifabhängige Ermittlung mindestens einer Abgabegebühr entsprechend des vorgenannten Verbrauchswertes, Bildung einer Nachricht, welche mindestens die Abgabegebühr einschließt, Sichern der Nachricht mittels eines Überprüfungscodes, Aufzeichnung einer Mitteilung (m1), welche die Nachricht und den Überprüfungscode enthält, Kommunikation mit einem entfernten Server (2), zur Übermittlung der kryptographisch gesicherten Nachricht in Form eines ersten Datensatzes (D1).

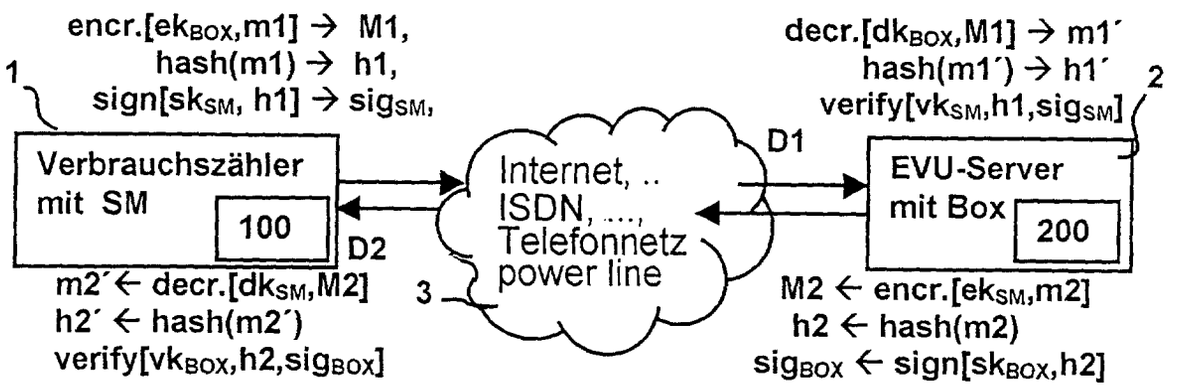

Fig. 4

EP 1 246 135 A2

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zur Aufzeichnung eines Verbrauchswertes, gemäß der im Oberbegriff des Anspruchs 1 angegebenen Art und einen Verbrauchszähler mit einem Meßwertgeber, gemäß der im Oberbegriff des Anspruchs 10 angegebenen Art. Der Verbrauchszähler hat einen Sicherheitsmodul zur Erhöhung der Fälschungssicherheit. Ein solcher kann in Verbrauchszählern und ähnlichen Geräten eingesetzt werden, die in einer potentiell unfreundlichen Umgebung, beispielsweise in Maschinenbaubetrieben, in öffentlichen oder privaten Gebäuden, arbeiten.

[0002] Bei der Postbearbeitung, bei welcher ebenfalls eine hohe Fälschungssicherheit gefordert wird, kommen bereits kryptographische Sicherheitsmaßnahmen bei einer Abrechnung von Frankierungen und bei der Erzeugung einer für einen jeden Frankierabdruck einzigartigen Markierung zum Einsatz.

Unter dem Titel: "Methode and arrangement for generating and checking a security imprint" wurde bereits in der US 5.953.426 ein spezielles Secret Key Verfahren vorgeschlagen. Der geheime Schlüssel (Secret Key) wird in einer sicheren Datenbank an der Verifizierungsstelle, typischerweise bei der Postbehörde, aufgehoben und damit geheim gehalten. Aus den Daten einer zu übermittelnden Botschaft wird ein Data Authentication Code (DAC) gebildet, der in eine Markierungssymbolreihe umgesetzt wird, welche dann als sogenannte digitale Unterschrift zur Authentifikationsprüfung der Botschaft verwendet werden kann. Dabei wird der auch aus der US 3,962,539 bekannte Data Encryption Standard (DES)-Algorithmus angewendet. Letzterer ist der bekannteste symmetrische Kryptoalgorithmus. Mit einem symmetrischen Kryptoalgorithmus lassen sich bei Daten des o.g. DAC oder bei Mitteilungen ein Message Authentifications Code (MAC) erzeugen, wobei solche Code zur Authentifikationsprüfung verwendet werden. Beim symmetrischen Kryptoalgorithmus steht dem Vorteil eines relativ kurzen MAC's der Nachteil eines einzigen geheimen Schlüssel gegenüber.

[0003] Der Vorteil eines asymmetrischen Kryptoalgorithmuses wird durch einen öffentlichen Schlüssel begründet. Ein bekannter asymmetrischer Kryptoalgorithmus, der nach den Namen seiner Erfinder R.Rivest, A.Shamir und L. Adleman benannt und im US 4,405,829 beschrieben wurde, ist der RSA-Algorithmus. Bekanntlich entschlüsselt der Empfänger mit einem privaten geheimen Schlüssel eine verschlüsselte Nachricht, welche beim Sender mit einem öffentlichen Schlüssel verschlüsselt wurde. Der Empfänger hält seinen privaten Schlüssel geheim, aber verschickt den zugehörigen öffentlichen Schlüssel an potentielle Absender. RSA war das erste asymmetrische Verfahren, das sich sowohl zur Schlüsselübermittlung als auch auch zur Erstellung digitaler Unterschriften eignete.

[0004] Mit dem privaten Schlüssel lassen sich ebenfalls digitale Unterschriften erzeugen, wobei die öffentlichen Schlüssel zur Authentifikation der Signatur dienen. Sowohl RSA, wie auch digitale Signatur-Algorithmen benutzen zwei Schlüssel, wobei einer der beiden Schlüssel öffentlich ist. Der Schlüsseleinsatz erfolgt hierbei in der umgekehrten Reihenfolge. Die Implementation des RSA-Algorithmus in einem Computer ergibt aber eine außerordentlich langsame Abarbeitung und liefert eine lange Signatur.

Es wurde schon ein Digital Signatur Standard (DSS) entwickelt, der eine kürzere digitale Unterschrift liefert und zu dem der Digital Signatur Algorithm (DSA) nach US 5,231,668 gehört. Diese Entwicklung erfolgte ausgehend von der Identifikation und Signatur gemäß dem Schnorr-Patent US 4,995,085 und ausgehend vom Schlüsseltausch nach Diffie-Hellman US 4,200,770 bzw. vom ElGamal-Verfahren (El Gamal, Taher, "A Public Key Cryptosystem and a Signatur Scheme Based on Diskrete Logarithms", 1III Transactions and Information Theory, vol. IT-31, No. 4, Jul.1985). Beim asymmetrischen Kryptoalgorithmus steht dem Vorteil des Verwendens eines öffentlichen Schlüssels der Nachteil einer relativ langen digitalen Unterschrift gegenüber.

[0005] In der US 6.041.704 wurde unter dem Titel: "Methode for operating a digitally printing postage meter to generate and check a security imprint" vorgeschlagen, ein modifiziertes Public Key-Verfahren für eine kürzere Signatur zu verwenden. Jedoch ist nur mit außerordentlich schnellen Prozessoren eine außerordentlich lange andauernde Datenverarbeitung zu vermeiden. Um den geheimen privaten Schlüssel vor einem Diebstahl aus einem Computer oder aus einer Frankiermaschine zu schützen, muß ein Sicherheitsbereich geschaffen werden, denn die gesamte Sicherheit der Signatur beruht darauf, dass der private Schlüssel nicht bekannt wird. Der öffentliche Schlüssel könnte dagegen in einer Vielzahl von Postinstitutionen zur Überprüfung der Signatur verwendet werden. Ein solcher Sicherheitsbereich wird in Geräten durch einen sogenannten Sicherheitsmodul geschaffen. Nachteil ist, dass letzterer eine hohe Rechenleistung aufweisen muß, um in Echtzeit oder in einer vertretbaren Zeitdauer die Datenverarbeitung abzuschließen.

[0006] Die Datenverarbeitung einer Hash-Funktion ist dagegen sogar um zwei bis vier Größenordnungen schneller als die Datenverarbeitung der digitalen Signatur oder der asymmetrischen Verschlüsselung. Die Bildung einer Quersumme ist ein sehr einfaches Beispiel für eine Hash-Funktion. Die Bytefolge einer Information wird einerseits zu einen Hashwert komprimiert und andererseits unterscheidet sich der Hashwert von anderen Hashwerten, die aus anderen Informationen gebildet wurden. Bei den in der Kryptografie genutzten Einweg-Hashfunktionen ist es nahezu unmöglich eine andere Bytefolge zu bilden, die denselben Hashwert ergibt. Die Einweg-Hashfunktionen sollen generell nicht umkehrbar sein. Eine von Ron Rivest im Jahre 1991 entwickelte Einweg-Hashfunktionen MD5 hat einen 128 Bit langen Hashwert soll aber nicht so sicher sein wie MD160 oder SHA (Secure Hash Algorithm). Die beiden letzteren verwenden einen 160-Bit Hashwert. Der SHA wurde vom NIST unter Mitwirkung der NSA entwickelt und im Jahre 1994 publiziert.

Der SHA ist Bestandteil des Digital Signatur Algorithm (DAS). Die gesammelten Aufzeichnungen können zur Inspektion an eine dritte Stelle versandt bzw. gesendet werden. An jede individuelle Aufzeichnung könnte ein Message Authentication Code (MAC) angehängt werden. Das erfordert eine zentrale Speicherung eines Geheimschlüssels, welcher für jeden Sicherheitsmodul einzigartig ist.

Bei einer Frankiermaschine vom Typ JetMail® wird bereits ein Sicherheitsmodul (EP 1.035.513 A2, EP 1.035.516 A2, EP 1.035.517 A2, EP 1.035.518 A2) eingesetzt, das einen symmetrischen Kryptoalgorithmus nutzt. Eine Schlüsselübertragung zwischen dem Sicherheitsmodul und einer Datenzentrale erfolgt mittels einem DES-verschlüsselten Datensatz, welcher außerdem MAC-gesichert ist. Die kryptographische Berechnung ist aber nur eine der Sicherheitsmaßnahmen bei einer Abrechnung von Dienstleistungen und Berechnung einer Gebühr für die Abgabe der Dienstleistungen sowie bei einer Übermittung des Abrechnungsergebnisses bzw. der Buchung zu einer entfernten Datenzentrale. Ein Sicherheitsmodul muß auch einen physikalischen oder chemischen Angriff überstehen. Ein solcher Angriff kann ebenfalls detektiert und aufgezeichnet werden.

[0007] Aus der US 4,812,965 ist bereits ein System für ein entfernte Inspektion eines Gerätes bekannt geworden, welche das Erfordernis einer lokalen Inspektion reduziert. Jede Fälschungshandlung wird von dem Gerät aufgezeichnet und zu einer zentralen Station übermittelt. Jedoch schützt diese Lösung nicht gegen solche Angriffe, wie die "Man in the middle Atacke", die gestartet werden, wenn eine Information via Modem zur zentralen Station gesendet wird.

[0008] Im EP 504 843 B1 (US 5.243.654) wurde bereits ein Gebührenerfassungssystem mit aus der Ferne rückstellbarer Zeitsperre und mit einem Gerät vorgeschlagen, das zur Abgabe einer verbuchbaren Größe (Energie) ausgestattet ist, wobei der Benutzer eines Gerätes dazu gezwungen ist, dem Datenzentrum regelmäßig den Stand der Abrechnungsregister mitzuteilen. Nachteilig ist, dass kein Sicherheitsmodul vorhanden ist und dass ein Benutzer eine Kombination in das Gerät eingeben muß.

[0009] Als einzige Sicherheitsmaßnahme ist ein Siegel oder eine Plombe am Verbrauchszähler vorgesehen. Bei einer Umgehung dieser Sicherheitsmaßnahme kann die Aufzeichnung des Verbrauchswertes in Fälschungsabsicht manipuliert werden. Durch solche Manipulationen geht den (Energie-)Versorgungsunternehmen regelmäßig viel Geld verlohren. Während den Großkunden einerseits die Möglichkeit geboten wird, mit günstigen Tarifen legal Geld zu sparen, wird Kleinkunden andererseits kein Anreiz geboten, verbilligte Tarife zu nutzen. Dabei ist offensichtlich nur zu Spitzenzeiten des Verbrauches beispielsweise die Energie teuerer bzw. die Dienstleistung schwieriger zu erbringen, was dann natürlich dem Kunden des Dienstleistungs- oder Versorgungsunternehmens in berechtigter Weise in Rechnung gestellt wird.

[0010] Es ist Aufgabe, ein Verfahren zur Aufzeichnung eines Verbrauchswertes mit hoher Fälschungssicherheit zu schaffen, welche für den Kunden eine Gebührenabrechnung vereinfacht oder kostensparend durchzuführen gestattet und dass für eine automatische und sichere Kommunikation mit einem entfernten Server des Dienstleistungs- oder Versorgungsunternehmens geeignet ist.

[0011] Es ist weiterhin Aufgabe, einen Verbrauchszähler mit einem Meßwertgeber zu schaffen, wobei feststellt werden kann, wenn am Verbrauchszähler manipuliert wird. Durch eine Vielzahl an unterschiedlichen temporär gültigen Tarifen soll auch dem Kleinkunden gestattet werden, Geld einzuparen. Dabei soll der lokale Aufwand möglichst gering sein.

[0012] Die Aufgabe wird mit den Merkmalen des Anspruchs 1 für das Verfahren bzw. mit den Merkmalen des Anspruchs 10 für den Verbrauchszähler gelöst. Letzterer wird mit einem Sicherheitsmodul ausgestattet.

[0013] Ein Verbrauchszähler ist ein Gerät mit Zufuhr und Abgabe von Materie, Energie oder Information unter Ermittlung einer verbuchbaren Größe. Ein Sicherheitsmodul ist ein mit Sicherheitsmitteln ausgestattetes Aufzeichnungsmodul für die Buchung oder Abrechnung einer Abgabegebühr und für die Bildung einer Nachricht über die vorgenannte Aufzeichnung. Ein Verbrauchszahler wird mit einem Sicherheitsmodul und mit einem Kommunikationsmittel ausgestattet, wobei letzteres eine automatische und sichere Kommunikation mit einem entfernten Server des Dienstleistungsoder Versorgungsunternehmens gestattet. Die Ermittelung einer verbuchbaren Größe, wie beispielsweise die Energie in einem Energiezähler, erfordert eine Analog/Digital-Umwandlung mindestens einer analogen Meßgröße und eine Berechnung nach einem ersten mathematischen Algorithmus. Der Sicherheitsmodul ist mit einem internen A/D-Wandler und mit einem Mikroprozessor ausgestattet, der zur Berechnung nach dem ersten mathematischen Algorithmus programmiert ist. Die dienstleistungs- bzw. verbrauchswertabhängige Abrechnung einer Abgabegebühr, erfolgt basierend auf einer Echtzeit in temporär unterschiedlicher Weise. So können beispielsweise Tarife für Tag und Nacht, Werktags und Wochenende, Sommer und Winter unterschiedlich sein. Der Sicherheitsmodul ist mit einer internen batterie-versorgten Echtzeituhr und einer Abrechnungseinheit, zum Beispiel einer Hardwareabrechnungseinheit, ausgestattet. Nach Abrechnung der Abgabegebühr nach zugehörigen Tarif entsprechend der Verbrauchszeitdauer und der aktuellen Zeit erfolgt eine Bildung einer Nachricht zur Aufzeichnung mindestens der Abgabegebühr. Die Aufzeichnung kann neben der Abgabegebühr den Verbrauch, den zugehörigen Tarif, die Verbrauchszeitdauer und die aktuelle Zeit enthalten. Vorzugsweise am Ende jedes Zeitabschnittes der Verbrauchszeitdauer erfolgt die Sicherung der Aufzeichnung durch einen Authentisierungscode.

[0014] Die Zeitabschnitte werden periodisch und/oder ereignisbasierend gebildet. Der Sicherheitsmodul ist zur Be-

rechnung des Authentisierungscodes nach einem ersten kryptographischen Algorithmus programmiert. Der Sicherheitsmodul ist mit einem Watchdogtimer ausgestattet, der die Kommunikationsmittel regelmäßig für eine Kommunikation mit dem entfernten Server freischaltet. Ein gescheiterter Kommunikationversuch wird in Zeitabständen solange wiederholt, bis eine Verbindung zustande kommt oder bis ein Kreditrahmen überschritten ist. In dem letzteren Fall, wird der Verbrauchszähler für die Abgabe der Verbrauchswerte gesperrt. Der Server überwacht, ob im erwarteten Zeitrahmen vom Verbrauchszähler des Kunden eine Meldung eingegangen ist und ob letztere authentisch ist. Die Meldung enthält verschlüsselte und zusätzlich mit einer digitalen Signatur gesicherte Daten, welche mittels des Mikroprozessors nach einem zweiten kryptographischen Algorithmus verschlüsselt und nach einem dritten kryptographischen Algorithmus signiert werden. Der Mikroprozessor überwacht, ob an dem Verbrauchszähler oder am Sicherheitsmodul manipuliert wurde. Beispielsweise ist ein Sensor zur Ermittlung vorgesehen, ob der Verbrauchszähler illegal abgeklemmt oder via Bypass überbrückt wurde. Die Meldung an den Server enthält entsprechend gesicherte Sensordaten. Der Server kann die Abgabe des Verbrauchswertes in Auswertung der übermittelten Daten sperren.

[0015] Für die Meldung wird ein asymmetrisches Verschlüsselungsverfahren als zweiter kryptographischer Algorithmus eingesetzt, um einen verschlüsselten Datensatz mit Abgabe- bzw. Verbrauchswerten, Zeitdaten, Sensordaten ggf. Schlüsseln u.a. Daten auszutauschen. Geeignet ist beispielsweise das RSA-Verfahren, wobei beim Absender ein Datensatz mit einem Public Key des Empfängers verschlüsselt wird. Beim Empfänger erfolgt eine Entschlüsselung des verschlüsselten Datensatzes erfolgt mit dem zugehörigen Privat Key des Empfängers.

[0016] Ein digitalen Signatur basierend auf einem dritten kryptographischen Algorithmus erfolgt beispielsweise mit dem umgekehrten RSA-Verfahren, wobei beim Absender ein gehashter Datensatz mit einem Privat key des Absenders verschlüsselt wird und beim Empfänger mit dem zugehörigen Public Key des Absenders entschlüsselt wird. Der auf vorgenannte Weise wiedergewonnene gehashte Datensatz wird mit einem gehashten Vergleichsdatensatz verglichen. Der Vergleichsdatensatz wird beim Empfänger aus dem verschlüsselten Datensatz durch Entschlüsselung und Anwendung der gleichen Hash-Funktion erzeugt. Bei Übereinstimmung des wiedergewonnenen gehashten Datensatzes mit dem gehashten Vergleichsdatensatz gilt die vom Server empfangene Meldung als authentisch und die übermittelten Werte werden gespeichert.

[0017] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Figur 1, Darstellung eines bekannten RSA-Verfahrens,

Figur 2, Darstellung eines Signier-Verfahrens unter Anwendung von RSA,

Figur 3, Darstellung des Schlüsseltausches,

Figur 4, Darstellung des Systems für eine kryptigraphisch gesicherte Kommunikation,

Figur 5, Darstellung eines Verbrauchszählers,

Figur 6, Blockschaltbild eines Energieverbrauchszählers,

Figur 7, Blockschaltbild eines Sicherheitsmoduls.

[0018] In der Figur 1 wird der Flußplan eines Public Key-Verfahrens am Beispiel von RSA erläutert. Die Anwendung asymmetrischer Verschlüsselungsalgorithmen (RSA, ElGamal) erfordert die Generierung eines Schlüsselpaares:

$$(ek, dk) \leftarrow genKey(k). \quad (1)$$

[0019] Ein Verschlüsselungsschlüssel ek ist öffentlich und ein Entschlüsselungsschlüssel dk ist privat. Der öffentliche Verschlüsselungsschlüssel ek, n wird zum Teilnehmer am Absendeort einer Mitteilung übermittelt. Dabei ist beispielsweise durch einen authentischen Kanal oder ein Zertifikat zu sichern, dass der öffentliche Verschlüsselungsschlüssel nicht zwischen Bestimmungsort und Absendeort ausgetauscht wird und im Rahmen einer "man in the middle attack" mißbraucht wird. Zur Verschlüsselung der Mitteilung m am Absendeort zum Chiffriertext c ist eine mathematische Operation vorgesehen:

$$c \leftarrow encrypt\ (ek, m) \quad (2)$$

[0020] Bei RSA kommt eine sogenannte modulare Arithmetik bzw. Kongruenzrechnung zum Einsatz. Zwei natürliche Zahlen a und c heißen kongruent modulo n, wenn a und c den gleichen Rest bei einer Teilung durch n lassen. Man setzt $a = m^{ek}$ und erhält zum Beispiel: $c \equiv m^{ek} \pmod{n}$

[0021] Der Chiffriertext c kann nun über einen ungesicherten Kanal zum Bestimmungsort übermittelt werden. Zur Entschlüsselung des Chiffriertextes c ist eine Operation vorgesehen:

$$m \leftarrow \text{decrypt}(dk, c) \tag{3}$$

[0022] Der zweite Teilnehmer am Bestimmungsort entschlüsselt mit seinem privaten Entschlüsselungsschlüssel dk den Chiffriertext c zur Mitteilung: $m' \equiv c^{dk} \pmod{n}$. Letztere stimmt nach den Gesetzen der modularen Arithmetik mit der ursprünglichen Mitteilung m überein, wenn m' und c^{dk} kongruent modulo n. Es gilt somit: $m = m'$.

[0023] In der Figur 2 wird der Flußplan eines Signier-Verfahrens am Beispiel von RSA erläutert. Die Anwendung digitaler Signaturmechanismen (RSA, DSA oder ECDSA) erfordert ebenfalls die Generierung eines Schlüsselpaares. Zunächst wird ein öffentliche Verifizierschlüssel vk, n zum zweiten Teilnehmer am Bestimmungsort übermittelt, beispielsweise über einen authentischen Kanal oder ein Zertifikat gesichert. Ein Signierschlüssel sk verbleibt als privater Schlüssel des Sicherheitsmoduls am Absendeort eines ersten Teilnehmers und der Verifizierschlüssel vk ist als öffentlicher Schlüssel zum Auswerten von digitalen Signaturen sig vorgesehen, die einer Mitteilung m (= message) zugeordnet sind. Die Mitteilung m und die Signatur können nun über einen ungesicherten Kanal zum zweiten Teilnehmer am Bestimmungsort übermittelt werden. Zur Erzeugung einer Signatur sig durch den Sicherheitsmodul am Absendeort eines ersten Teilnehmers ist eine mathematische Operation vorgesehen:

$$sig \leftarrow \text{sign}(sk, m) \tag{4}$$

[0024] Zur Verringerung der Länge einer Signatur sig wird zunächst auf die Mitteilung m eine Hash-Funktion angewendet:

$$h = \text{hash}(m) \tag{5}$$

[0025] Zum Signieren am Absendeort eines ersten Teilnehmers kommt ein privater Signierschlüssel sk des Sicherheitsmoduls und beispielsweise wieder die sogenannte modulare Arithmetik bzw. Kongruenzrechnung zum Einsatz:

$$sig \equiv h^{sk} \pmod{n} \tag{6}$$

[0026] Zur Verifizierung einer Signatur sig am Bestimmungsort ist ein öffentlicher Verifizierschlüssel vk, die unverschlüsselte Mitteilung m und eine mathematische Operation der Art vorgesehen:

$$acc \leftarrow \text{verify}(vk, m, sig). \tag{7}$$

wobei das Ergebnis wahr (gültig) oder falsch (ungültig) sein kann. Vor der Überprüfung wird auf die Mitteilung m eine Hash-Funktion angewendet:

$$h = \text{hash}(m) \tag{8}$$

[0027] Der zweite Teilnehmer verifiziert am Bestimmungsort mit dem öffentlichen Verifizierschlüsselungsschlüssel vk die Signatur sig zum Hashwert h', welcher nach den Gesetzen der modularen Arithmetik mit dem aus der ursprünglichen Mitteilung m gebildeten Hashwert h übereinstimmt, wenn h' und sig^{vk} kongruent modulo n sind. Es gilt somit:

$$h = h' \equiv sig^{vk} \pmod{n} \tag{9}$$

[0028] Für $h \neq h'$ gilt die Signatur sig oder Mitteilung m als nicht authentisch, aber anderenfalls für $h = h'$ als authen-

tisch.

[0029] Es ist vorgesehen, dass jeder Kommunikationsteilnehmer mit einem Sicherheitsmodul bzw. einer Sicherheitsbox ausgestattet wird, welche vor der Kommunikation, in welcher eine Übermittlung von Mitteilungen erfolgt, über einen authentischen Kanal öffentliche Schlüssel austauschen. Das kann vorzugsweise bei Verkäufer oder Händler des Sicherheitsmoduls geschehen oder beim Hersteller.

[0030] Anhand der in der Figur 3 gezeigten Darstellung wird der Schlüsseltausch zwischen einem Sicherheitsmodul und einer Sicherheitsbox näher erläutert. Zunächst wird jeweils in Beiden ein Schlüsselpaar generiert. Das Sicherheitsmodul SM generiert einen öffentlichen Verschlüsselungsschlüssel ek_{SM} und einen privaten Entschlüsselungsschlüssel dk_{SM}. Das Sicherheitsmodul SM generiert weiterhin einen öffentlichen Verifizierschlüssel vk_{SM} und einen privaten Signierschlüssel sk_{SM}. Die Sicherheitsbox BOX generiert einen öffentlichen Verschlüsselungsschlüssel ek_{BOX} und einen privaten Entschlüsselungsschlüssel dk_{BOX}. Die Sicherheitsbox BOX generiert weiterhin einen öffentlichen Verifizierschlüssel vk_{BOX} und einen privaten Signierschlüssel sk_{BOX}. Die öffentlichen Schlüssel werden zum jeweiligen Kommunikationsteilnehmer übermittelt. Von der Sicherheitsbox BOX 200 zum Sicherheitsmodul SM 100 werden der öffentliche Verschlüsselungsschlüssel ek_{BOX} und der öffentliche Verifizierschlüssel vk_{BOX} übermittelt und dort gespeichert. Von dem Sicherheitsmodul SM 100 zur Sicherheitsbox BOX 200 werden der öffentliche Verschlüsselungsschlüssel ek_{SM} und der öffentliche Verifizierschlüssel vk_{SM} übermittelt und dort gespeichert.

[0031] In der Figur 4 wird eine Darstellung des Systems für eine kryptigraphisch gesicherte Kommunikation über einen ungesicherten Kanal gezeigt. Der Verbrauchszählers 1 ist mit dem EVU-Server 2 via ISDN, DECT-Telefon, Internet, power line oder ein anderes Netz verbunden. Der Verbrauchszähler 1 hat ein Sicherheitsmodul SM 100, welches zur Ver-/Entschlüssellung einer Mitteilung m mit einem öffentlichen Verschlüsselungsschlüssel ek_{BOX} der Sicherheitsbox BOX 200 ausgestattet ist. Nach einem auf den Gleichungen (2) bzw. (5) basierenden zweiten kryptographischen Algorithmus wird erst ein Chiffriertext M1 gebildet und auf die Mitteilung m eine Hash-Funktion angewendet, wobei der Hashwert $h1 \leftarrow hash(m)$ entsteht. Nach einem auf den Gleichungen (4) und (5) basierenden dritten kryptographischen Algorithmus wird vom Sicherheitsmodul SM 100 eine Signatur $sig_{SM} \leftarrow sign[sk_{SM},h1]$ gebildet. Der Chiffriertext M1 und die digitale Signatur sig_{SM} werden als Datensatz D1 = M1, sig_{SM} zur Sicherheitsbox des EVU-Servers 2 übermittelt. Der EVU-Server 2 entschlüsselt mit seinem privaten Entschlüsselungsschlüssel dk_{BOX} den Chiffriertext M1 zur Mitteilung m1 und überprüft deren Echtheit anhand der Signatur. Der EVU-Server 2 erzeugt eine Mitteilung m2 übermittelt in einem Datzensatz D2 die zum Chiffriertext M2 verschlüsselte Mitteilung an den Sicherheitsmodul. Die Mitteilung m2 kann einen Freischaltcode für den Verbrauchszähler 1 einschließen. Die Mitteilung m1 enthält Verbrauchs- und Buchungsdaten bzw. Abgabewerte und Abrechnungswerte, Zeitdaten u.a. Daten. Sie kann vom EVU-Server weiter ausgewertet werden, um eine Abrechnung entsprechend dem gültigen Tarif zu erzeugen. Der zum Sicherheitsmodul SM 100 übermittelte Datensatz D2 enthält ebenfalls einen Chiffriertext M2 und die digitale Signatur sig_{BOX}. Mittels der letzteren wird die Echtheit des Freischaltcodes verifizierbar. Beim Empfangen des kryptographisch gesicherten Freischaltcodes in Form eines zweiten Datesatzes D2 erfolgt eine Aufzeichnung der Änderung durch Rücksetzen der Abgabegebühr auf Null, wenn der Freischaltcode echt war. Andernfalls wird der Verbrauchszähler gesperrt.

[0032] Die Figur 5 zeigt eine Darstellung eines Verbrauchszählers, zum Beispiel eines Strom- bzw. Energiezählers 1. Letzterer ist zwischen ein Stromkabel 8 und ein Hausstromkabel 6 geschaltet und mit einer Anzeigeeinheit 4 für den Energieverbrauch ausgestattet. Ein Sicherheitsgehäuse 10 des Strom- bzw. Energiezählers 1 ist mit einem Sicherheitsschloss 9 ausgestattet. Weitere Besonderheiten sind ein Fenster 7 für eine zusätzliche Statusanzeige des Sicherheitsmoduls (nicht sichtbar) und ein optionales Kabel 5 für eine Kommunikationsverbindung mit einem EVU-Server zum Beispiel via ISDN-Telefonnetz.

[0033] Die Figur 6 zeigt ein Blockschaltbild eines Energiezählers 1. Letzterer könnte einen üblichen Haushaltszähler (Induktionszähler für Einphasenwechselstrom mit Ferrarismesswerk) ersetzen. Am Sicherheitsmodul könnte zur Detektion einer Manipulation der Schalter S1 angeschlossen werden, der beim Öffnen des Sicherheitsgehäuses 10 ebenfalls geöffnet wird. Die Statusanzeige mittels LED 107, 108 signalisiert ein unbefugtes Öffnen auch nach dem Wiederschliessen des Sicherheitsgehäuses 10. Hardwareseitig ist ein Auslöseschalter S2 für das Zurücksetzen angeschlossen. Er wird z.B. bei Schalten des Sicherheitsschlosses 9 in eine zweite Schaltstellung ausgelöst. Ein Zurücksetzen des Status des SM 100 ist nur einem beauftragten Inspektor erlaubt, der einen entsprechenden Schlüssel besitzt und eine Kommunikation mit dem EVU-Server auslöst, um die Inspektion anzumelden bzw. mitzuteilen. Handelsübliche Messwertgeber 104, 105 für Strom- oder Spannungsmessung liefern nach Vollweggleichrichtung ein analoges Mess-Signal i(t), u(t), welches per DA-Wandler 102, 103 in ein digitales Signal gewandelt und dann an die Dateneingänge des Sicherheitsmoduls SM 100 angelegt wird. Die Momentanwerte derjenigen gleichgerichteten Spannung u(t), die beispielsweise an einem Lastwiderstand R abfällt oder die sich aufgrund einer magnetischen Induktion für eine Induktivität L bei einem Laststrom i ergibt $u(t) = L \cdot di/dt$, werden unter Verwendung eines Multiplexers vom Mikroprozessor des SM 100 abgetastet, wenn zwei Dateneingänge wechselseitig abgetastet werden müssen. Nach Abtastung der Dateneingänge und einer digitalen Multiplikation der Mess-Signale $u(t) \cdot i(t)$ erfolgt eine Aufsummierung für eine jede halbe Periode T/2 des Einphasenwechselstromes. Durch diese Momentanwertmultiplikation und zusammen mit einer kumulativen Abspeicherung der Summen der Beträge ergibt sich die wirksame Leistung P im Zeitbereich $\Delta t = x \cdot T$. Die

jeweiligen Momentanwerte werden in einem nichtflüchtigen Speicher addiert und das abgespeicherte Ergebnis oder ein Momentanwert können angezeigt werden. Entsprechende Datenausgänge des Sicherheitsmoduls SM 100 sind für die Anzeigeeinheit 4 vorgesehen. Es sei t1 der Beginn und t2 das Ende des Zeitbereiches Δt_1 = t2 - t1, der eine Vielzahl x von Perioden T einschließt, wobei ein erster Tarif für die Abrechnung einer Abgabegebühr F1 gültig ist. Weiterhin sei t3 der Beginn und t4 das Ende eines zweiten Zeitbereiches Δt_2 = t4 - t3, der ebenfalls eine Vielzahl x von Perioden T einschließt, wobei ein zweiter Tarif für die Abrechnung einer Abgabegebühr F2 gültig ist. Bei einem Ereignis, wie Tarif- oder Lastwechsel, erfolgt durch den Mikroprozessor eine Berechnung der Abgabegebühr nach dem zugehörigen Tarif entsprechend der Verbrauchszeitdauer und eine Speicherung in separaten Speicherbereichen der nichtflüchtigen Speicher zusammen mit dem jeweils zugehörigen aktuellen Verbrauchswert V_K. Eine weitere Abspeicherung von Nutzdaten kann erfolgen, um das Benutzerverhalten zu ermitteln bzw. um Marketingdaten abzuleiten.

[0034] Vom Sicherheitsmodul wird ein Ereignis V_K zum Zeitpunkt tj festgestellt, welches mindestens als Echtzeitnachricht aufgezeichnet werden muß. Hinzukommen weitere Daten, beispielsweise eine tarifabhängige Abgabegebühr. Solche Datenelemente sind zum Beispiel:

#K: Sequenzzähler ('13'),
R: Typbezeichner der Nachricht ('R' für Realtime),
$V1_K$: Verbrauchs- und Nutzdaten ('Tages-Verbrauch,Mr. Pauschinger'),
$F1_K$: Abgabegebühr nach erstem Tarif ('Tages-Verbrauchsgebühr'),
$V2_K$: Verbrauchs- und Nutzdaten ('Nacht-Verbrauch,Mr. Pauschinger'),
$F2_K$: Abgabegebühr nach zweitem Tarif ('Nacht-Verbrauchsgebühr'),
t_j: aktueller Echtzeitwert (dezimalisiert: '8491028108032001') mit fester Länge,
A_K: Authentisierungscode (dezimalisiert : '8023024892048398'), i.e. Unterschrift, typischerweise mit fester Länge,

[0035] Im ersten Schritt vor der ersten kryptographischen Operation erfolgt eine Zusammenstellung einer 'Realtime'-Nachricht $V1_K$, $F1_K$, $V2_K$, $F2_K$, t_j mit weiteren Daten #K, R, zum Bilden eines Datensatzes:

$$INPUT = \#K, R, V1_K, F1_K, V2_K, F2_K, t_j \tag{10}$$

zum Beispiel sei #K = 13 für eine 13.Aufzeichnung:

[0036] INPUT = '13RTages-Verbrauch,Mr.PauschingerTages-Verbrauchsgebühr Nacht-Verbrauch,Mr.Pauschinger-Nacht-Verbrauchsgebühr 8491028108032001

[0037] Im zweiten Schritt erfolgt aus INPUT durch Bildung des Hashwertes eine Berechnung des Authentisierungscodes A_K.

$$A_K \leftarrow hash(INPUT) \tag{11}$$

[0038] Zum Beispiel:

A_K = '8023024892048398'.

[0039] Im dritten Schritt erfolgt ein Anfügen des resultierenden Authentisierungscodes A_K an die Echtzeitnachricht. Zum Zeitpunkt t_j lautet die Mitteilung m1 mit der zu speichenden Nachricht also:

$$m1 = \#K, R, V1_K, F1_K, V2_K, F2_K, t_j, A_K \qquad \text{mit } K = 13 \tag{12}$$

[0040] Ein Aufzeichnen umfaßt ein Speichern von Echtzeit- und Gebührendaten. Periodisch erfolgt ein Übertragen eines Datensatzes D1 vom Sicherheitsmodul am Absendeort zu einer Sicherheitsbox eines EVU-Servers am Bestimmungsort.

[0041] Zur Vorbereitung der Erzeugung einer digitalen Signatur wird die Mitteilung m1 gehasht:

$$h1 \leftarrow hash(m1) \tag{13}$$

[0042] In dem Sicherheitsmodul 100 liegen ein öffentlicher Verschlüsselungsschlüssel ek_{BOX} der Box und ein privater Signierschlüssel sk_{SM} des Sicherheitsmoduls 100 nichtflüchtig eingespeichert vor. Durch ein im internen Programmspeicher gespeichertes Programm ist der Mikroprozessor des Sicherheitsmoduls 100 programmiert, als Authentifika-

tionsmaschine zu arbeiten. Die digitalen Signatur wird mit dem Signierschlüssel sk_{SM} des Sicherheitsmoduls SM 100 gebildet:

$$sig_{SM} \leftarrow sign[sk_{SM},h1] \quad (14)$$

[0043] Zur Vorbereitung der Übermittelung der Nachricht an den Server 2 verschlüsselt der Mikroprozessor des Sicherheitsmoduls SM 100 die Mitteilung m1 mit dem Verschlüsselungschlüssel ek_{BOX} der Sicherheitsbox zum Chiffriertext M1:

$$M1 \leftarrow encrypt[ek_{BOX}, m1] \quad (15)$$

[0044] Der zu übermittelnde Datensatz D1 lautet:

$$D1 = M1, sig_{SM} \quad (16)$$

[0045] Jeder Verbrauchszähler 1 enthält eine Kommunikationseinheit 101 für eine Kommunikation mit dem Server 2, der eine vergleichbare Kommunikationseinheit (nicht gezeigt) aufweist. In der Sicherheitsbox 200 des Servers 2 liegen ein privater Entschlüsselungsschlüssel dk_{BOX} der Box und ein öffentlicher Verifizierschlüssel vk_{SM} des Sicherheitsmoduls 100 nichtflüchtig eingespeichert vor. Durch ein im internen Programmspeicher gespeichertes Programm ist der Mikroprozessor der Sicherheitsbox 200 programmiert, als Verifikationsmaschine zu arbeiten. Der Server 2 arbeitet angepaßt an die jeweilige Art und Weise der Erzeugung der Aufzeichnung. Wonach der durch den Server 2 aus dem Sicherheitsmodul 100 abgerufene Aufzeichnungsstrom analysiert wird, hängt von der entsprechenden Anwendung ab.

[0046] Die Figuren 5 und 6 zeigen ein am Verbrauchszähler 1 angeschlossenes ISDN-Kabel 5. Es ist für ein Ausführungsbeispiel vorgesehen, dass die Kommunikationseinrichtung 101 ein Modem vorzugsweise ein ISDN-Modul ist, welches über ein Telefon-/ISDN-Netz mit dem Server 2 kommunikativ verbunden ist. Bei Kommunikation des Verbrauchszählers 1 mit dem EVU-Server 2 direkt via ISDN-Netz kann eine entsprechende Kommunikationseinheit 101 aus dem Telefon-/ISDN-Netz oder über eine Leitung 106 vom Netzteil oder vom Hausstromkabel 6 mit Energie versorgt werden.

Alternativ ist es möglich, einen vorhandenen Digital-Powerline-Dienst des Enegieversorgungsunternehmens (EVU) zu nutzen. Die Kommunikationseinrichtung 101 ist nun ein Power-line-Modul, der über ein Enegierversorgungsnetz mit dem Server 2 kommunikativ verbunden ist. Der Power-line-Modul ist entsprechend ausgebildet eine Nachricht mit Übertragungsraten bis zu 1Mbit/s über eine Leitung 106 via Stromkabel 8 zum EVU-Server 2 zu übertragen. Dabei werden die vorhandenen Stromversorgungskabel als physikalisches Trägermedium für ein Kommunikationsnetzwerk genutzt. Dabei entfällt natürlich das o.g. ISDN-Kabel 5.

Eine weitere Alternative zur Vermeidung von Kabelverbindungen bietet ein 2,4 GHz Bluetooth-Funkempfänger/Sender-Baustein, der als Kommunikationseinrichtung 101 eingesetzt wird. Es ist vorgesehen, dass die Kommunikationseinrichtung 101 im Sicherheitsmodul 100 integriert ist. Ein Blue-Tooth-Modul, der drahlos über einen weiteren Blue-Tooth-Modul mit dem Server 2 kommunikativ verbunden werden soll, kann aber nur über relativ kurze Entfernungen ca. 10 m mit einem gleichen Bluetooth-Baustein kommunizieren, so dass letzterer doch wieder an ein ISDN-Endgerät angeschlossen ist. Somit ist der weitere Blue-Tooth-Modul wieder über ein Telefonnetz mit dem Server 2 kommunikativ verbunden. Zum Beispiel wird wieder das ISDN-Netz genutzt.

Das Sicherheitsmodul SM 100 kann über das Hausstromkabel 6 oder das Stromkabel 8 aus dem Energienetz mit Energie versorgt werden. Dazu ist ein Netzteil N 109 erforderlich, welches vorzugsweise so angeschlossen ist, daß der Stromkunde die Kosten trägt. Der Masseanschluß an Pin P23 erhält zum Beispiel das negative und der Betriebsspannungsanschluß an Pin P25 das positive Spannungspotential. Ein Elektrolytkondensator C puffert die Betriebsspannung. An den Anschlüssen P1, P2 liegt eine Leiterschleife, die sich über das gesamte Sicherheitsgehäuse erstreckt und beim Zerstören des Sicherheitsgehäuses 10 unterbrochen wird. Es ist vorgesehen, dass der Verbrauchszähler 1 ein Sicherheitsgehäuse 10 aufweist, welches den Sicherheitsmodul 100, eine Anzeigeeinheit 4 eine Zuführ- und Abgabeeinrichtung 8, 6 und eine Kommunikationseinrichtung 101 umschließt. Der Sicherheitsmodul 100 ist mit mindestens einem Meßwertgeber 104, 105, mit der Anzeigeeinheit 4 zur Anzeige eines Verbrauchswertes sowie mit Sicherheitsmitteln S1, S2, 18 verbunden. Der Sicherheitsmodul 100 weist einen nichtflüchtigen Speicher 124, 129 zur Speicherung temporär gültiger Tarife auf und ist programmiert, eine Abgabegebühr basierend auf dem Verbrauchswert tarifabhängig zu berechnen und auf ein Ansprechen der Sicherheitsmittel S1, S2, 18 sowie auf Werte der Meßwertgeber

104, 105 zu reagieren, welche eine Manipulation in Fälschungsabsicht signalisieren. Das Sicherheitsmodul enthält intern eine Lithium-Batterie 134 zur Datenerhaltung der nichtflüchtig gespeicherten Daten, um eine Notversorgung bei Energieausfall zu ermöglichen. Bei den nichtflüchtig gespeicherten Daten wird zusätzlich zur kumulierten Leistung auch die Zeit gespeichert, so daß eine Abtrennung vom Energieversorgungsnetz nachträglich unterschieden werden kann vom Spannungsausfall im Energieversorgungsnetz. Das Sicherheitsmodul SM 100 schaltet bei fehlender Systemspannung einfach auf Notversorgung via Batterie 134 um.

Der Sicherheitsmodul 100 nimmt die Funktion eines Spannungswächters wahr, um zu überprüfen, ob der Zähler abgeklemmt wurde oder nicht. Der Verbrauchszähler 1 hat mindestens einen Analog/Digital-Wandler 102, 103, der mit dem mindestens einen Meßwertgeber 104, 105 verbunden ist. Alternativ hat der Sicherheitsmodul 100 einen Analog/Digital-Wandler 127 integriert, der mit den Meßwertgebern 104, 105 verbunden ist. Der Sicherheitsmodul 100 weist einen Echtzeitzähler 122 auf und der Sicherheitsmodul 100 nimmt die Funktion eines Watch dog Timers wahr, um regelmäßig Zählerstände an einen Server 2 zu übermitteln. Dadurch dass das Sicherheitsmodul 100 einen Echtzeitzähler 122 aufweist, kann der Mikroprozessor des Sicherheitsmoduls 100 auf den temporär gültigen Tarif zugreifen, der im nichtflüchtigen Speicher gespeichert ist. Der Mikroprozessor des Sicherheitsmoduls 100 ist programmiert, eine Abgabegebühr basierend auf dem Verbrauchswert tarifabhängig zu berechnen.

[0047] Die Figur 7 zeigt ein Blockschaltbild eines verbesserten Sicherheitsmoduls SM 100. Beim unberechtigten Öffen des Sicherheitsgehäuses und /oder entfernen des Sicherheitsmoduls 100 wird der Schalter S1 betätigt und eine Detektionseinheit 13 speichert das Ereignis nichtflüchtig. Bei einer Beschädigung des Sicherheitsgehäuses 10, beispielsweise durch Bohren in das Sicherheitsgehäuse, wird eine an die Pins P1 und P2 angeschlossenen Leiterschleife 18 geöffnet, über welche im geschlossenen Zustand zeitlich zuordenbare Impulse übermittelt werden. Der Mikroprozessor empfängt die gesendeten Impulse zwecks Auswertung der Detektionsdaten hinsichtlich einer Beschädigung bzw. Manipulation am Sicherheitsgehäuse 10. Ein ordnungsgemäßes Öffnen/Schließen des Sicherheitsgehäuses 10 wird mittels Auslöseschalter S2 detektiert. Die Schalter S1, S2 und die Leiterschleife 18 liegen an Ein/Ausgängen eines Ein/Ausgangsinterfaces 125 des Mikroprozessors 120.

Als geeigneter Mikroprozessor µP 120 eignet sich der Typ S3C44A0X von Firma Samsung vor. Letzterer weist zusätzlich Analogeingänge für Analogwerte u(t), i(t), einen internen Multiplexer (nicht gezeigt) und einen internen AD-Wandler 127 auf, so dass separate AD-Wandler entfallen können. An den Analogeingängen werden 4 Leitungen für die Analogwerte u(t), i(t) angeschlossen. Außerdem wird mittels integriertem LCD-Controller (nicht gezeigt) eine am Ein/Ausgangsinterface 125 angeschlossene externe LCD-Anzeige 4 unterstützt. Am Ein-/Ausgangsinterface 125 sind externe Leuchtdioden 107, 108 zur Zustandsanzeige angeschlossen. Der Status des Sicherheitsmoduls 100 kann vorteilhaft über eine Bicolor-Leuchtdiode anstelle der Leuchtdioden 107, 108 signalisiert werden. Eine Statusmeldung kann weitere Datenelemente umfassen, zum Beispiel:

- Detektionsdaten einer Manipulation am Gehäuse,
- Detektionsdaten einer Manipulation am Sicherheitsmodul,
- Versionsnummer und Gültigkeitsdatum der Tarife,
- Spitzenlast und Uhrzeit der Spitzenbelastung,
- Nächster Kommunikationstermin usw.

[0048] Mit den 60-bit general purpose I/O ports stehen genügend Ein/Ausgänge am Mikroprozessor 120 zur Verfügung, um eine Kommunikationseinheit 101 und weitere E/A-Mittel direkt anzuschliessen. Vorteilhaft wird jedoch eine Anpassungslogig in Form des ASIC 150 und der programmierbaren Logik 160 zwischen Mikroprozessor 120 und Kommunikationseinheit 101 geschaltet. Die Kommunikationseinheit 101 kann in das Sicherheitsmodul SM 100 integriert und ggf. als ASIC ausgeführt werden. Hierzu eignet sich die moderne digitale Kommunikationtechnik, zum Beispiel ein Bluetooth-Modul. Letzterer gibt eine Sendeleistungen von ca. 1mW über eine kurze Antenne 51 ab. Die integrierte Echtzeituhr (Real Time Counter) 122 des Mikroprozessors 120 übernimmt neben den oben beschriebenen Sicherheitsfunktionen auch die Taktung der Kommunikation. Die Sicherheitsmodule 100 der Verbrauchszähler unterschiedlicher Kunden können an unterschiedlichen Tagen zur Kommunikation programmiert sein, so dass nicht alle gleichzeitig beim Server anrufen.

[0049] Der EVU-Server 2 übermittelt ggf. neue aktuelle Tarife, einschließlich Versionsnummer und Gültigkeitsdatum der Tarife, zwecks Speicherung im Sicherheitsmodul. Der Mikroprozessor hat hierzu ein internes RAM 124, welches batteriegestützt ist. Wenn letzteres nicht ausreicht, wird ein weiteres batteriegestütztes SRAM 129 in den Sicherheitsmodul integriert und arbeitet zusätzlich zum RAM 124 des Mikroprozessors 120, zwecks nichtflüchtiger Speicherung von Tarifwerten, die in vorbestimmten Zeitbereichen gültig sind. Die integrierte Echtzeituhr 122 liefert Echtzeitdaten. Der Mikroprozessor 120 übernimmt die Auswertung von Zeitdaten zur tarifabhängigen Ermittlung mindestens eines Verbrauchswertes. Bei vorbestimmten Ereignissen greift eine CPU 121 des Mikroprozessors 120 auf den temporär gültigen Tarif im SRAM 129 zu, wobei letzteres die Daten für die Abgabegebühr einer als ASIC 150 ausgebildeten Datenverarbeitungseinheit übergibt. Die Abrechnung erfolgt via ASIC 150 in den nichtflüchtigen Speichern NVRAM

114, 116. Für beide NVRAMs werden aus Sicherheitsgründen zwei unterschiedliche Speichertechnologien eingesetzt. In ereignis- und zeitbestimmten Zeitabständen erfolgt zur Abrechnung eine Bildung einer Nachricht, welche den Verbrauchswert, die Abgabegebühr und die Zeitdaten einschließt, eine Bildung eines Überprüfungscodes und Sichern der Nachricht mittels des Überprüfungscodes. Der Überpüfungscode wird von der CPU des Mikroprozessors 120 berechnet. Der ASIV 150 nimmt eine Bildung und Aufzeichnung einer Mitteilung m1 vor, welche die Nachricht und den Überprüfungscode enthält. In einer andereren Variante können Aufgaben des ASIC's vom Mikroprozessor 120 übernommen werden. Es ist vorgesehen, dass die Sicherung der Aufzeichnung des Verbrauchs vorzugsweise am Ende jedes Zeitabschnittes der Verbrauchszeitdauer erfolgt, wobei die Zeitabschnitte periodisch und/oder ereignisbasierend gebildet werden. Ein Eeignis ist beispielsweise ein Tarif- oder Lastwechsel.

[0050] In größeren Zeitabständen führt der Mikroprozessor 120 eine kryptographisch Sicherung einer Nachricht und eine Kommunikation mit einem entfernten Server 2 durch, zur Übermittlung der kryptographisch gesicherten Nachricht in Form eines ersten Datensatzes D1. Die Sicherheitsbox 200 des Servers 2 verrifiziert und entschlüsselt die Nachricht. Nur wenn eine Verifizierung die Echtheit der Nachricht ergibt, wird vom Server 2 ein Freischaltcode erzeugt. Die Sicherheitsbox 200 des Servers 2 kann den Freischaltcode durch Verschlüsseln und Signieren sichern. Der Sicherheitsmodul 100 des Verbrauchszählers 1 kann die Echtheit des Freischaltcodes anhand der Signatur des Servers 2 verifizieren. Es ist vorgesehen, dass beim Empfangen des kryptographisch gesicherten Freischaltcodes eine Aufzeichnung der Änderung der Abgabegebühr durch Rücksetzen auf Null erfolgt, wenn der Freischaltcode echt war sowie dass Sperren der Abgabe einer verbuchbaren Größe bzw. des Verbrauches eines Verbrauchswertes vorgenommen wird, wenn der Freischaltcode unecht ist.

[0051] Ein Verbrauch an festen, flüssigen oder gasförmigen Größen erfordert speziell angepaßte Zähler, die in erfindungsgemäßer Weise ebenfalls mit dem Sicherheitsmodul ausgestattet werden. In einem weiteren Einsatzfall ist der Verbrauchszähler eine Frankiermaschine. Die verbuchbare Größe ist dann der Frankierwert. Weitere Ausführungen zu weiteren Baugruppen des Sicherheitsmoduls sind den Veröffentlichungen EP 1.035.513 A2, EP 1.035.516 A2, EP 1.035.517 A2, EP 1.035.518 A2, DE 20020635 U1 zu entnehmen. Die Auswertung der Überwachungsfunktionen und kryptographischen Berechnungen erfolgen im Mikroprozessor. Der erste kryptographische Algorithmus für die Erzeugung des Authentisierungscodes für Aufzeichnungsdaten ist beispielsweise eine Hashfunktion. Natürlich kann anstelle des Authentisierungscodes auch eine Checksumme oder ein nach einem symmetrischen Verschlüsselungsalgorithmus gebildeter MAC eingesetzt werden. Natürlich kann auch die Abrechnungsfunktion des ASIC's 150 vom Mikroprozessor 120 übernommen oder überprüft werden.

[0052] Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die - vom gleichen Grundgedanken der Erfindung ausgehend - von den anliegenden Schutzansprüchen umfaßt werden.

Patentansprüche

1. Verfahren zur Aufzeichnung eines Verbrauchswertes, der in Auswertung von Meßwerten ermittelt wird, umfassend die Schritte:

   - nichtflüchtige Speicherung von Tarifwerten, die in vorbestimmten Zeitbereichen gültig sind,
   - Liefern und Verarbeitung von Meßwerten über die Zufuhr und Abgabe von Materie, Energie oder Information, wobei deren Verarbeitung nach einem ersten mathematischen Algorithmus erfolgt,
   - Liefern und Auswerten von Zeitdaten zur zeitabhängigen Ermittlung mindestens eines Verbrauchswertes bezogen auf Materie, Energie oder Information,
   - tarifabhängige Ermittlung mindestens einer Abgabegebühr entsprechend des vorgenannten Verbrauchswertes,
   - Bildung einer Nachricht, welche mindestens die Abgabegebühr einschließt,
   - Bildung eines Überprüfungscodes und Sichern der Nachricht mittels des Überprüfungscodes,
   - Bildung und Aufzeichnung einer Mitteilung (m1), welche die Nachricht und den Überprüfungscode enthält,
   - Aufnahme einer Kommunikation mit einem entfernten Server (2), zur Übermittlung der kryptographisch gesicherten Nachricht in Form eines ersten Datensatzes (D1).

2. Verfahren, nach Anspruch 1, **gekennzeichnet durch** Wiederholung der Aufnahme einer Kommunikation mit einem entfernten Server (2), zur Übermittlung der kryptographisch gesicherten Nachricht in Form eines ersten Datensatzes (D1), und bei erfolgloser Wiederholung solange, bis ein Kreditrahmen überschritten ist, sowie Empfangen eines, nach dem Überprüfen der Echtheit des ersten Datensatzes (D1) vom Server (2) übermittelten, kryptographisch gesicherten Freischaltcodes in Form eines zweiten Datensatzes (D2), Überprüfen der Echtheit des Freischaltcodes anhand der Signatur des Servers (2) und Aufzeichnung des Ereignisses.

3. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** die gebildete Nachricht den Verbrauchswert, die Abgabegebühr und Zeitdaten einschließt, dass die Sicherung der Nachricht und die Aufzeichnung des Verbrauchs vorzugsweise am Ende jedes Zeitabschnittes der Verbrauchszeitdauer erfolgt, wobei die Zeitabschnitte periodisch und/oder ereignisbasierend gebildet werden.

4. Verfahren, nach Anspruch 2, **dadurch gekennzeichnet, dass** beim Empfangen des kryptographisch gesicherten Freischaltcodes eine Aufzeichnung der Änderung der Abgabegebühr durch Rücksetzen auf Null erfolgt, wenn der Freischaltcode echt war sowie dass ein Sperren der Abgabe einer verbuchbaren Größe bzw. des Verbrauches eines Verbrauchswertes vorgenommen wird, wenn der Freischaltcode unecht ist.

5. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** eine Analog/Digital-Wandlung der Meßwerte vor deren Verarbeitung erfolgt, wobei deren Verarbeitung eine Aufzeichnung einschließt, dass bei einem Ereignis eine Berechnung der Abgabegebühr nach dem zugehörigen Tarif entsprechend der Verbrauchszeitdauer und bei der Aufzeichnung eine Speicherung der Abgabegebühr zusammen mit dem jeweils zugehörigen aktuellen Verbrauchswert V_K erfolgt.

6. Verfahren, nach Anspruch 5, **dadurch gekennzeichnet, dass** das Ereignis ein Tarif- oder Lastwechsel ist.

7. Verfahren, nach Anspruch 3, **dadurch gekennzeichnet, dass** bei der Aufzeichnung eine weitere Abspeicherung von Nutzdaten erfolgt, um das Benutzerverhalten zu ermitteln bzw. um Marketingdaten abzuleiten.

8. Verfahren, nach Anspruch 1, **dadurch gekennzeichnet, dass** der Überprüfungscode ein Authentisierungscode ist.

9. Verfahren, nach Anspruch 8, **dadurch gekennzeichnet, dass** der Authentisierungscode ein Hashcode oder ein nach einem symmetrischen Verschlüsselungsalgorithmus gebildeter MAC ist.

10. Verbrauchszähler, mit einem Meßwertgeber, **dadurch gekennzeichnet, dass** der Verbrauchszähler (1) ein Sicherheitsgehäuse (10) aufweist, welches einen Sicherheitsmodul (100), eine Zuführ- und Abgabeeinrichtung (8, 6) und eine Kommunikationseinrichtung (101) umschließt, wobei der Sicherheitsmodul (100) mit mindestens einem Meßwertgeber (104, 105) sowie mit Sicherheitsmitteln (S1, S2, 18) verbunden ist, dass der Sicherheitsmodul (100) einen nichtflüchtigen Speicher (124, 129) zur Speicherung temporär gültiger Tarife aufweist und programmiert ist, eine Abgabegebühr basierend auf dem Verbrauchswert tarifabhängig zu berechnen und auf ein Ansprechen der Sicherheitsmittel (S1, S2, 18) sowie auf Werte der Meßwertgeber (104, 105) zu reagieren, welche eine Manipulation in Fälschungsabsicht signalisieren.

11. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** der Verbrauchszähler (1) mindestens einen Analog/Digital-Wandler (102, 103) aufweist, der mit dem mindestens einen Meßwertgeber (104, 105) verbunden ist und dass der Sicherheitsmodul (100) eine Überwachungsfunktion aufweist, um zu überprüfen, ob der Zähler abgeklemmt wurde oder nicht.

12. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (100) einen Analog/Digital-Wandler (127) aufweist, der mit den Meßwertgebern (104, 105) verbunden ist und dass der Sicherheitsmodul (100) eine Überwachungsfunktion aufweist, um zu überprüfen, ob der Zähler abgeklemmt wurde oder nicht.

13. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (100) einen Echtzeitzähler (122) aufweist und dass der Sicherheitsmodul (100) die Funktion eines Watch dog Timers aufweist, um regelmäßig Zählerstände an einen Server (2) zu übermitteln.

14. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** das Sicherheitsmodul (100) einen Echtzeitzähler (122) aufweist und dass ein Mikroprozessor (120) des Sicherheitsmoduls (100) auf den temporär gültigen Tarif zugreift, der im nichtflüchtigen Speicher (124, 129) gespeichert ist und programmiert ist, eine Abgabegebühr basierend auf dem Verbrauchswert tarifabhängig zu berechnen.

15. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** die Kommunikationseinrichtung (101) ein ISDN-Modul ist, der über ein Telefonnetz mit dem Server (2) kommunikativ verbunden ist.

16. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** die Kommunikationseinrichtung (101) ein Power-line-Modul ist, der über ein Enegierversorgungsnetz mit dem Server (2) kommunikativ verbunden ist.

17. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** die Kommunikationseinrichtung (101) ein Blue-Tooth-Modul ist, der drahlos über einen weiteren Blue-Tooth-Modul mit dem Server (2) kommunikativ verbunden ist.

18. Verbrauchszähler, nach Anspruch 17, **dadurch gekennzeichnet, dass** der Blue-Tooth-Modul drahlos mit einem weiteren Blue-Tooth-Modul verbunden ist, wobei letzterer über ein Telefonnetz mit dem Server (2) kommunikativ verbunden ist.

19. Verbrauchszähler, nach Anspruch 10, **dadurch gekennzeichnet, dass** die Kommunikationseinrichtung (101) im Sicherheitsmodul (100) integriert ist.

20. Verbrauchszähler, nach den Ansprüchen 10 bis 19, **dadurch gekennzeichnet, dass** der Verbrauchszähler (1) eine Frankiermaschine ist.

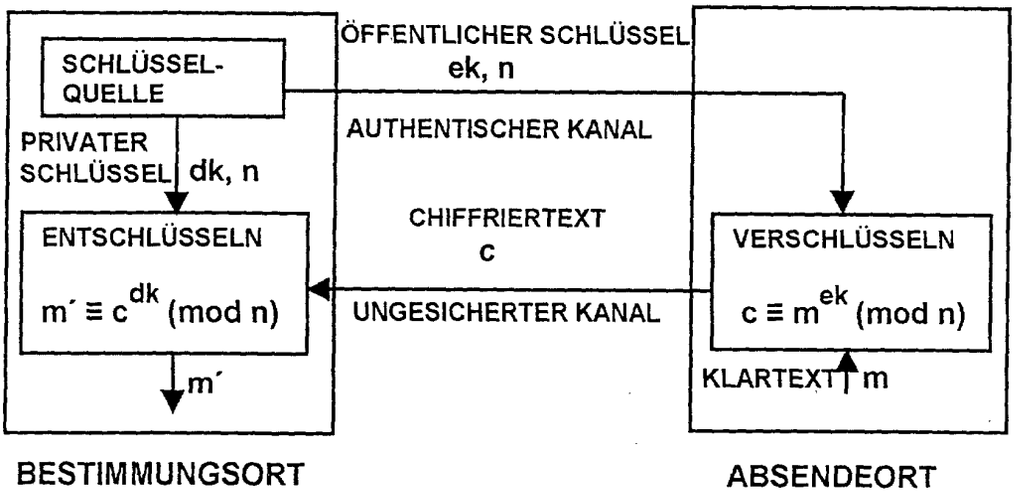

Fig. 1

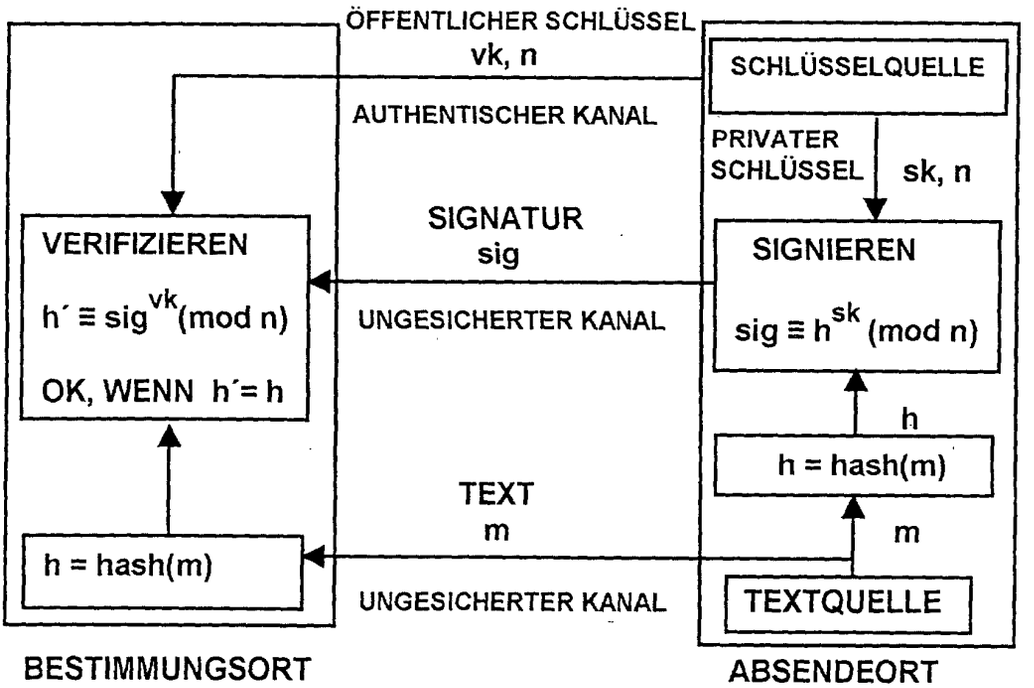

Fig. 2

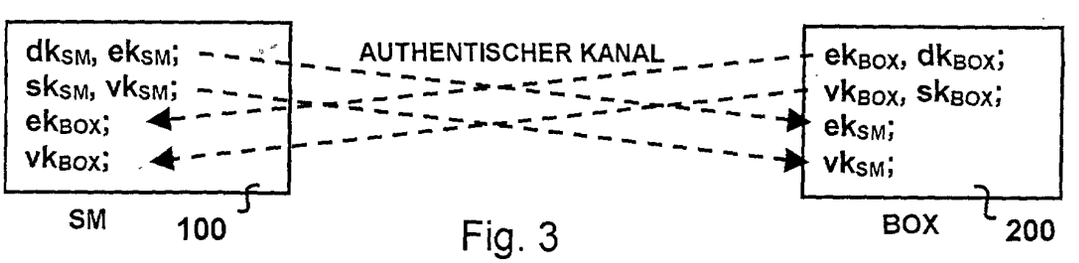

Fig. 3

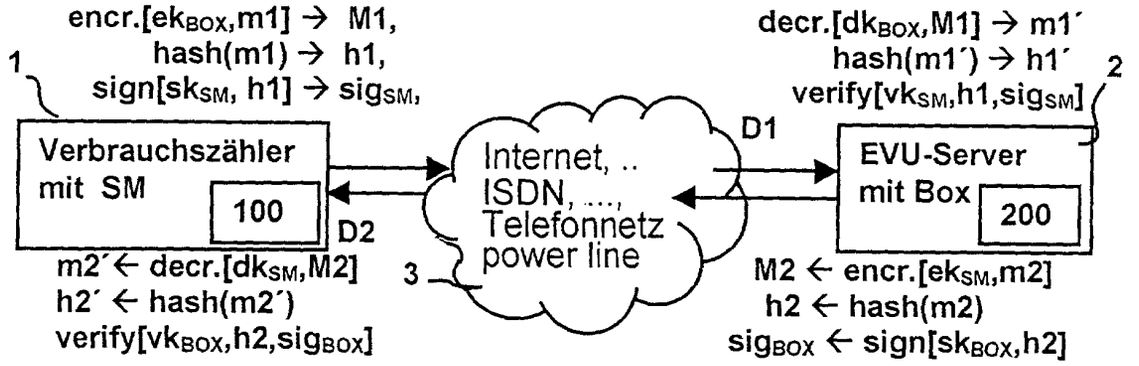

Fig. 4

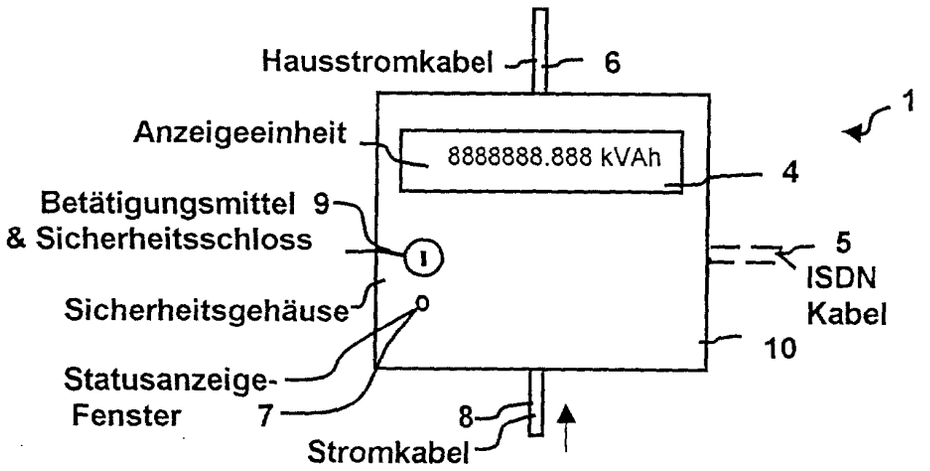

Fig. 5

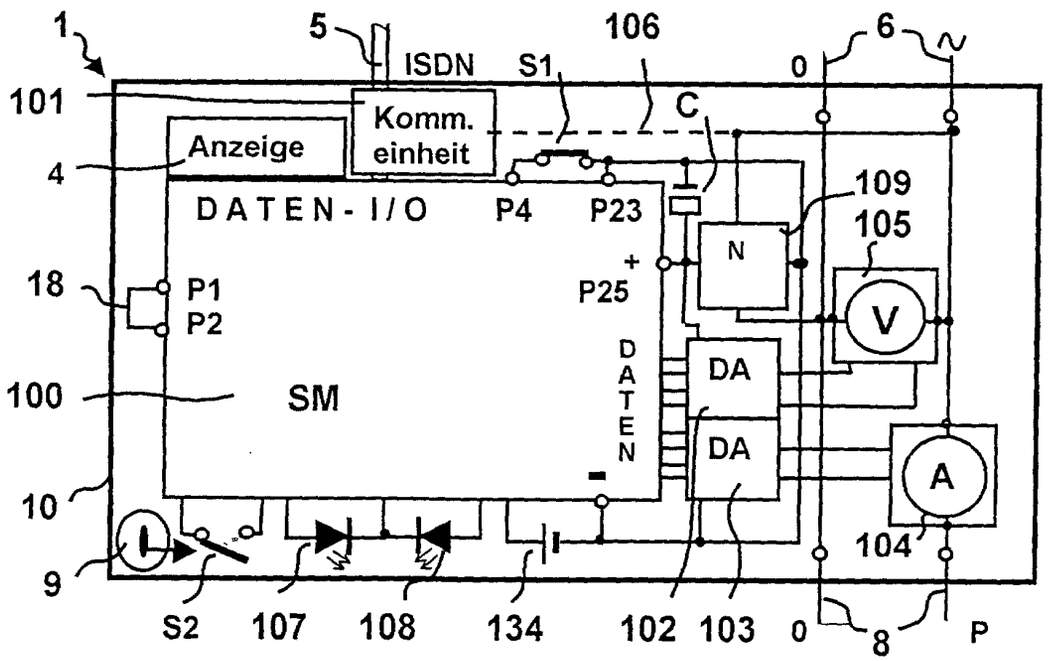

Fig. 6

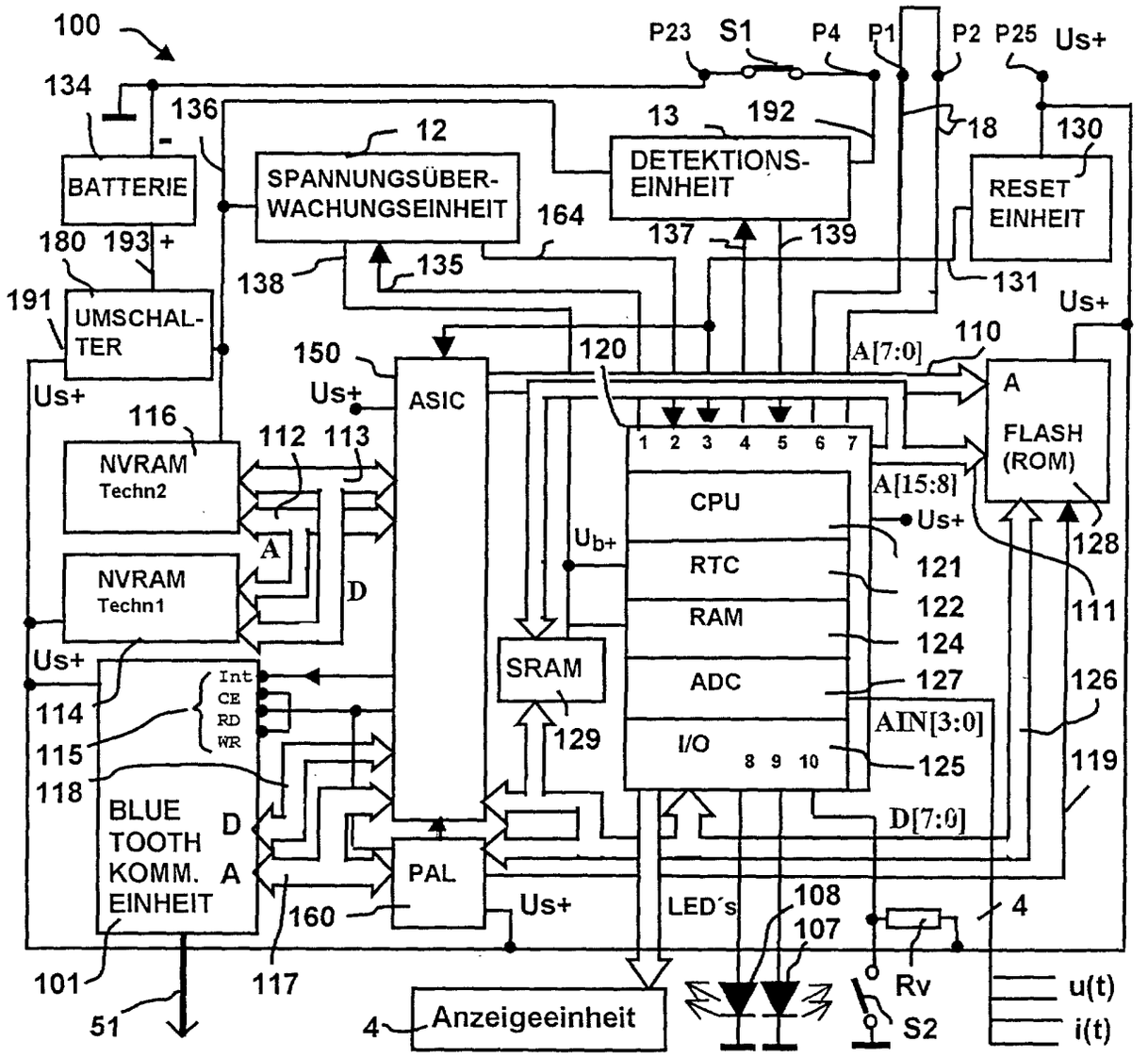
100
134
136
BATTERIE
180
193
+
191
UMSCHAL-
TER
Us+
116
NVRAM
Techn2
NVRAM
Techn1
A
D
Us+
114
115
118
Int
CE
RD
WR
BLUE
TOOTH
KOMM.
EINHEIT
D
A
101
51
117
12
SPANNUNGSÜBER-
WACHUNGSEINHEIT
138
135
164
150
Us+
ASIC
112
113
SRAM
129
PAL
160
Us+
4
Anzeigeeinheit
P23
S1
P4
P1
P2
P25
Us+
13
192
DETEKTIONS-
EINHEIT
137
139
18
130
RESET
EINHEIT
131
Us+
120
A[7:0]
110
A
FLASH
(ROM)
128
111
1 2 3 4 5 6 7
CPU
A[15:8]
Us+
121
RTC
122
RAM
124
ADC
127
I/O
8 9 10
125
AIN[3:0]
126
119
D[7:0]
Ub+
LED´s
108
107
4
Rv
S2
u(t)
i(t)

Fig. 7