(19) österreichisches patentamt

(10) **AT 510 067 B1 2012-04-15**

(12) **Patentschrift**

(21) Anmeldenummer: A 1143/2010
(22) Anmeldetag: 06.07.2010
(45) Veröffentlicht am: 15.04.2012

(51) Int. Cl. : ***G07F 7/00*** (2006.01)
G07B 15/00 (2006.01)
G06Q 20/00 (2006.01)

(56) Entgegenhaltungen:
EP 1069539A2 EP 1705595A2
GB 2423853A GB 2460240A
US 2003066883A1
US 2004003260A1
US 2007022472A1
WO 200229738A2

(73) Patentinhaber:
A1 TELEKOM AUSTRIA
AKTIENGESELLSCHAFT
A-1020 WIEN (AT)
RESEARCH INDUSTRIAL SYSTEMS
IT-ENGINEERING (RISE) FORSCHUNGS-,
ENTWICKLUNGS- UND
GROSSPROJEKTBERATUNG GMBH
A-2320 SCHWECHAT (AT)

(54) **VERFAHREN ZUM VALIDIEREN ELEKTRONISCHER TICKETS**

(57) Verfahren zum Validieren elektronischer Tickets (2), die von einer Zentrale (1) an mobile Endgeräte (3) gesandt und auf einer Anzeige (4) derselben angezeigt werden, mit Hilfe eines mobilen Kontrollgeräts (5), mit den Schritten Erzeugen eines elektronischen Tickets (2) und eines Paares (7) einander zugehöriger Schlüssel (S1, S2) in der Zentrale (1) , Verschlüsseln eines Bestandteils (b) des Tickets (2) mit Hilfe des einen Schlüssels (S1) des Paars (7) zu einer Validierungskomponente (B) des Tickets (2), Senden des Tickets (2) an das Endgerät (3) und des anderen Schlüssels (S2) an das Kontrollgerät (5), Eingeben eines benutzerwählbaren temporären Schlüssels (S3) in das Endgerät (3), Verschlüsseln der Validierungskomponente (B) des Tickets (2) im Endgerät (3) mit Hilfe des temporären Schlüssels (S3), Anzeigen der verschlüsselten Validierungskomponente (B*) auf dem Endgerät (3) und Einlesen (14) der verschlüsselten Validierungskomponente (B*) von der Anzeige (4) des Endgeräts (3) in das Kontrollgerät (5), Eingeben des temporären Schlüssels (S3) in das Kontrollgerät (5), und Entschlüsseln der verschlüsselten Validierungskomponente (B*) im Kontrollgerät (5) mit Hilfe des anderen Schlüssels (S2) des Paares (7) und des temporären Schlüssels (S3) , wobei die erfolgreiche Entschlüsselung das Ticket (2) validiert.

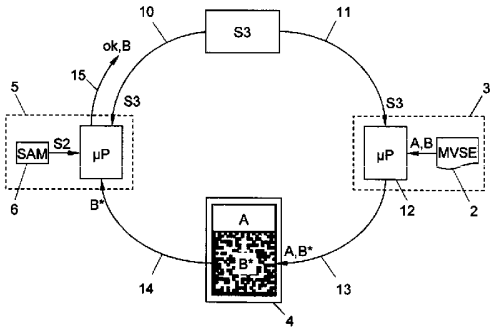

Fig.2

AT 510 067 B1 2012-04-15

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Validieren elektronischer Tickets, die von einer Zentrale an mobile Endgeräte gesandt und auf einer Anzeige derselben angezeigt werden, mit Hilfe eines mobilen Kontrollgeräts.

[0002] Auf mobilen Endgeräten, z.B. Mobiltelephonen, anzeigbare elektronische Tickets setzen sich in zunehmendem Maße als Eintrittskarten, Fahrausweise, Parkscheine usw. durch. Diese Tickets werden beispielsweise mittels SMS oder mobilen Internetverbindungen auf das Endgerät geladen und dort angezeigt und können so einer Kontrollperson zur Überprüfung der Echtheit bzw. Gültigkeit (Validierung) vorgewiesen werden. Das angezeigte Ticket kann beispielsweise im Klartext vorliegen oder ein maschinenlesbarer Code sein, z.B. ein Barcode. Um Betrugsversuche möglichst hintanzuhalten, werden Verschlüsselungstechniken angewandt, welche jedoch bislang nicht verhindern können, daß ein elektronisches Ticket kopiert und weitergegeben wird, z.B. mittels SMS von einem Mobiltelephon an ein anderes zur neuerlichen Anzeige („Replay") weitergesandt wird.

[0003] Die Erfindung setzt sich zum Ziel, ein Verfahren zum Validieren von elektronischen Tickets zu schaffen, das gegen solche Betrugsversuche weitgehend immun ist und erhöhte Daten- bzw. Validierungssicherheit bietet.

[0004] Dieses Ziel wird mit einem Verfahren der einleitend genannten Art erreicht, welches die folgenden Schritte umfaßt:

[0005] Erzeugen eines elektronischen Tickets und eines Paares einander zugehöriger Schlüssel in der Zentrale,

[0006] Verschlüsseln eines Bestandteils des Tickets mit Hilfe des einen Schlüssels des Paars zu einer Validierungskomponente des Tickets,

[0007] Senden des Tickets an das Endgerät und des anderen Schlüssels an das Kontrollgerät,

[0008] Eingeben eines benutzerwählbaren temporären Schlüssels in das Endgerät,

[0009] Verschlüsseln der Validierungskomponente des Tickets im Endgerät mit Hilfe des temporären Schlüssels,

[0010] Anzeigen der verschlüsselten Validierungskomponente auf dem Endgerät und Einlesen der verschlüsselten Validierungskomponente von der Anzeige des Endgeräts in das Kontrollgerät,

[0011] Eingeben des temporären Schlüssels in das Kontrollgerät,

[0012] und

[0013] Entschlüsseln der verschlüsselten Validierungskomponente im Kontrollgerät mit Hilfe des anderen Schlüssels des Paares und des temporären Schlüssels, wobei die erfolgreiche Entschlüsselung das Ticket validiert.

[0014] Auf diese Weise wird mit Hilfe zweier Schlüssel, von denen der eine - als Teil eines Schlüsselpaars - dem Kontrollgerät zugeordnet ist und der andere für jeden Validierungsvorgang beliebig gewählt werden kann, eine ständig wechselnde, für jeden Validierungsvorgang neue Validierungskomponente auf dem Engerät angezeigt. Diese Validierungskomponente ist nur mit dem entsprechenden, mit dem anderen Teil des Schlüsselpaars ausgestatteten Kontrollgerät und in Kenntnis des gewählten temporären Schlüssels entschlüsselbar, um das Ticket zu validieren. Dadurch ist ein Kopieren des angezeigten Tickets, d.h. seiner Validierungskomponente, für einen Betrüger wertlos, weil der temporäre Schlüssel bei jeder Validierungsabfrage ein anderer ist. Im Ergebnis wird damit Sicherheit gegenüber Replay-Attacken erreicht.

[0015] Eine bevorzugte Ausführungsform der Erfindung zeichnet sich durch den weiteren Schritt des Anzeigens der entschlüsselten Validierungskomponente auf dem Kontrollgerät aus. Dadurch bildet der Inhalt der Validierungskomponente einen dritten Sicherheitsaspekt: Ihr Inhalt

kann zur zusätzlichen Überprüfung herangezogen werden, wenn es sich um Daten handelt, die eine Kontrollperson von einem gültigen Ticket erwartet.

[0016] Besonders günstig ist es, wenn das Ticket als weiteren Bestandteil eine Darstellungskomponente enthält, welche auf dem Endgerät neben der verschlüsselten Validierungskomponente angezeigt wird. Dadurch kann eine Vorprüfung des Tickets - schon vor dem Einlesen der Validierungskomponente - anhand der Darstellungskomponente vorgenommen werden, welche beispielsweise grundlegende Daten des Tickets wie Gültigkeitsort und -zeit in Klartext wiedergibt.

[0017] Besonders günstig ist es, wenn die verschlüsselte Validierungskomponente auf der Anzeige des Endgeräts als Barcode angezeigt und mittels eines Barcodelesers des Kontrollgeräts in dieses eingelesen wird, was eine rasche Verarbeitung ermöglicht. Bevorzugt wird ein zweidimensionaler Barcode verwendet, mit welchem ein hoher Informationsgehalt selbst auf kleinen Bildschirmen von mobilen Endgeräten dargestellt werden kann.

[0018] Gemäß einer weiteren bevorzugten Ausführungsform der Erfindung ist das Schlüsselpaar ein Public/Private-Key-Schlüsselpaar. Wenn beispielsweise der an das Kontrollgerät gesandte Schlüssel der Public-Key des Paars ist, kann dadurch selbst aus der Kenntnis des Schlüssels im Kontrollgerät nichts gewonnen werden.

[0019] Grundsätzlich könnte das elektronische Ticket auf beliebige Art und Weise von der Zentrale an die mobilen Endgeräte gesandt werden, beispielsweise auf einem Offline-Datenträger. Bevorzugt erfolgt das Senden des Tickets von der Zentrale an das Endgerät in an sich bekannter Weise über ein Mobilfunknetz, was hohe Akzeptanz und Komfort für den Benutzer bietet.

[0020] Die Erfindung wird nachstehend anhand eines in den beigeschlossenen Zeichnungen dargestellten Ausführungsbeispiels näher erläutert. In den Zeichnungen zeigt:

[0021] Fig. 1 einen ersten Teil des erfindungsgemäßen Verfahrens umfassend das Erzeugen und Verteilen der Schlüssel und elektronischen Tickets; und

[0022] Fig. 2 einen zweiten Teil des erfindungsgemäßen Verfahrens umfassend das Validieren eines Tickets auf einem mobilen Endgerät mit Hilfe eines mobilen Kontrollgeräts.

[0023] In Fig. 1 ist eine Zentrale 1 zum Erzeugen von sicheren elektronischen Tickets 2 gezeigt, im weiteren auch als „mobile Virtual secure elements" (MVSE) bezeichnet. Die Tickets 2 werden von der Zentrale 1 an mobile Endgeräte 3 (Fig. 2) gesandt, und zwar auf beliebige Art und Weise, z.B. über das Internet, über physische Offline-Datenträger, oder bevorzugt über ein Mobilfunknetz, z.B. in Form einer Kurznachricht (SMS). Das mobile Endgerät 3 kann von beliebiger Art sein, beispielsweise ein Mobiltelefon, Personal Digital Assistant (PDA), Notebook, Laptop usw. Das Endgerät 3 verfügt über eine Anzeige 4, auf der eine, mehrere oder alle Komponenten des elektronischen Tickets 2 angezeigt werden können, wie später noch ausführlicher erläutert wird.

[0024] Die auf der Anzeige 4 angezeigten Daten werden zur Validierung des Tickets 2 mit Hilfe eines mobilen Kontrollgeräts 5 verarbeitet. Diese Daten können auf beliebige Art und Weise in das Kontrollgerät 5 eingegeben werden, z.B. drahtlos über eine Funkschnittstelle wie RFID, NFC, Bluetooth, WLAN usw., manuell durch Ablesen durch eine Kontrollperson und Eingeben in eine Tastatur des Kontrollgeräts 5, oder durch optisches Scannen der Anzeige 4 mit einem Scanner, z.B. einem OCR- oder Barcodereader bzw. -Scanner.

[0025] Zur Verarbeitung der Daten des Tickets 2 verfügt das Kontrollgerät 5 über ein Kryptographiemodul 6 („secure access module", SAM). Bei der Generierung der Tickets 2 erzeugt die Zentrale 1 ein Schlüsselpaar 7 aus einem ersten Schlüssel S1 und einem zugehörigen zweiten Schlüssel S2, und zwar, einerseits für die an die Endgeräte 3 zu verteilenden Tickets 2 und anderseits für eine beliebige Anzahl von Kontrollgeräten 5. Der eine Schlüssel S1 wird dazu verwendet, in der Zentrale 1 einen Bestandteil b des Tickets 2 zu einer sog. Validierungskomponente B zu verschlüsseln, und der andere Schlüssel S2 wird direkt in den Kryptographiemo-

dulen 6 der Kontrollgeräte 5 hinterlegt. Die Schlüssel S1, S2 des Schlüsselpaars 7 können ihrerseits von einem Master-Schlüssel S abgeleitet sein, der von an einer Applikation 8 erzeugt wird, welche einen Auftrag 9 zur Generierung eines Satzes von Tickets 2 unter dem Masterschlüssel S an die Zentrale 1 erteilt.

[0026] Die Tickets 2 können neben der Validierungskomponente B als weiteren Bestandteil eine unverschlüsselte Komponente A, eine sog. Darstellungskomponente enthalten, welche beispielsweise Klartext-Daten des Tickets wie Gültigkeitszeit und -ort, Aussteller, Einlöseort usw. enthalten.

[0027] Nachdem die Tickets 2 mit der unverschlüsselten Darstellungskomponente A und der mit dem Schlüssel S1 verschlüsselten Validierungskomponente B an die Endgeräte 3 und die Schlüssel S2 an die Kontrollgeräte 5 verteilt wurden, kann die Validierung eines bestimmten Tickets 2 wie in Fig. 2 dargestellt durchgeführt werden. Eine Kontrollperson am Kontrollgerät 5 wählt einen beliebigen temporären Schlüssel S3, z.B. eine kurze Ziffernfolge, und gibt diese sowohl in das Kontrollgerät 5 (Schritt 10) als auch das Endgerät 3 (Schritt 11) ein bzw. veranlaßt sie den Besitzer des Endgeräts 3, den temporären Schlüssel S3 in das Endgerät 3 einzugeben. Im Endgerät 3 verschlüsselt ein Prozessor 12 die Validierungskomponente B des Tickets 2 mit Hilfe des temporären Schlüssels S3 und gibt die verschlüsselte Validierungskomponente, hier mit B* bezeichnet, auf der Anzeige 4 des Endgeräts 3 aus (Schritt 13). Gegebenenfalls kann zusätzlich die Darstellungskomponente A mit ausgegeben werden.

[0028] Im Schritt 14 wird die verschlüsselte Validierungskomponente B* von der Anzeige 4 des Endgeräts 3 in das Kontrollgerät 5 eingelesen, sei es auf drahtlosem Wege, manuell durch Benutzereingabe in das Kontrollgerät 5 oder durch OCR- oder Barcode-Scannen, sofern die verschlüsselte Validierungskomponente B* als Barcode dargestellt wird.

[0029] Im Kontrollgerät 5 wird anschließend die verschlüsselte Validierungskomponente B* mit Hilfe des im Kryptographiemodul 6 hinterlegten Schlüssels S2 und des zuvor in Schritt 10 eingegebenen temporären Schlüssels S3 wieder entschlüsselt. Eine erfolgreiche Entschlüsselung („ok") validiert das Ticket 2; optional kann dabei der Inhalt der Validierungskomponente B auf dem Kontrollgerät 5 angezeigt werden, falls diese Nutzdaten enthält (Schritt 15).

[0030] Die verschlüsselte Validierungskomponente B* wird auf der Anzeige 4 bevorzugt als zweidimensionaler Barcode angezeigt. Die Schlüssel S1, S2 des Schlüsselpaars 7 können ident sein; bevorzugt ist das Schlüsselpaar 7 jedoch ein Public/Private-Key-Schlüsselpaar, wobei der im Kryptographiemodul 6 des Kontrollgeräts 5 hinterlegte Schlüssel S2 der Public-Key des in der Zentrale 1 verwendeten Private-Key S1 ist. Es versteht sich, daß die hier erörterten Schlüssel S1, S2 auch in Form von Zertifikaten vorliegen können, die beispielsweise von einem Master-Zertifikat(Schlüssel) S der Applikation 8 abgeleitet sein können.

[0031] Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt, sondern umfaßt alle Varianten und Modifikationen, die in den Rahmen der angeschlossenen Ansprüche fallen.

Patentansprüche

1. Verfahren zum Validieren elektronischer Tickets, die von einer Zentrale an mobile Endgeräte gesandt und auf einer Anzeige derselben angezeigt werden, mit Hilfe eines mobilen Kontrollgeräts, mit den Schritten

   Erzeugen eines elektronischen Tickets (2) und eines Paares (7) einander zugehöriger Schlüssel (S1, S2) in der Zentrale (1),

   Verschlüsseln eines Bestandteils (b) des Tickets (2) mit Hilfe des einen Schlüssels (S1) des Paars (7) zu einer Validierungskomponente (B) des Tickets (2),

   Senden des Tickets (2) an das Endgerät (3) und des anderen Schlüssels (S2) an das Kontrollgerät (5),

   Eingeben eines benutzerwählbaren temporären Schlüssels (S3) in das Endgerät (3),

   Verschlüsseln der Validierungskomponente (B) des Tickets (2) im Endgerät (3) mit Hilfe des temporären Schlüssels (S3),

   Anzeigen der verschlüsselten Validierungskomponente (B*) auf dem Endgerät (3) und Einlesen (14) der verschlüsselten Validierungskomponente (B*) von der Anzeige (4) des Endgeräts (3) in das Kontrollgerät (5),

   Eingeben des temporären Schlüssels (S3) in das Kontrollgerät (5), und

   Entschlüsseln der verschlüsselten Validierungskomponente (B*) im Kontrollgerät (5) mit Hilfe des anderen Schlüssels (S2) des Paares (7) und des temporären Schlüssels (S3), wobei die erfolgreiche Entschlüsselung das Ticket (2) validiert.

2. Verfahren nach Anspruch 1, **gekennzeichnet durch** den weiteren Schritt des Anzeigens (15) der entschlüsselten Validierungskomponente (B) auf dem Kontrollgerät (5).

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß das Ticket (2) als weiteren Bestandteil eine Darstellungskomponente (A) enthält, welche auf dem Endgerät (3) neben der verschlüsselten Validierungskomponente (B*) angezeigt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß die verschlüsselte Validierungskomponente (B*) auf der Anzeige (4) des Endgeräts (3) als Barcode angezeigt und mittels eines Barcodelesers des Kontrollgeräts (5) in dieses eingelesen wird.

5. Verfahren nach Anspruch 4, **dadurch gekennzeichnet**, daß der Barcode ein zweidimensionaler Barcode ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß das Schlüsselpaar (7) ein Public/Private-Key-Schlüsselpaar ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, daß das Senden von der Zentrale (1) an das Endgerät (3) über ein Mobilfunknetz erfolgt.

Hierzu 1 Blatt Zeichnungen

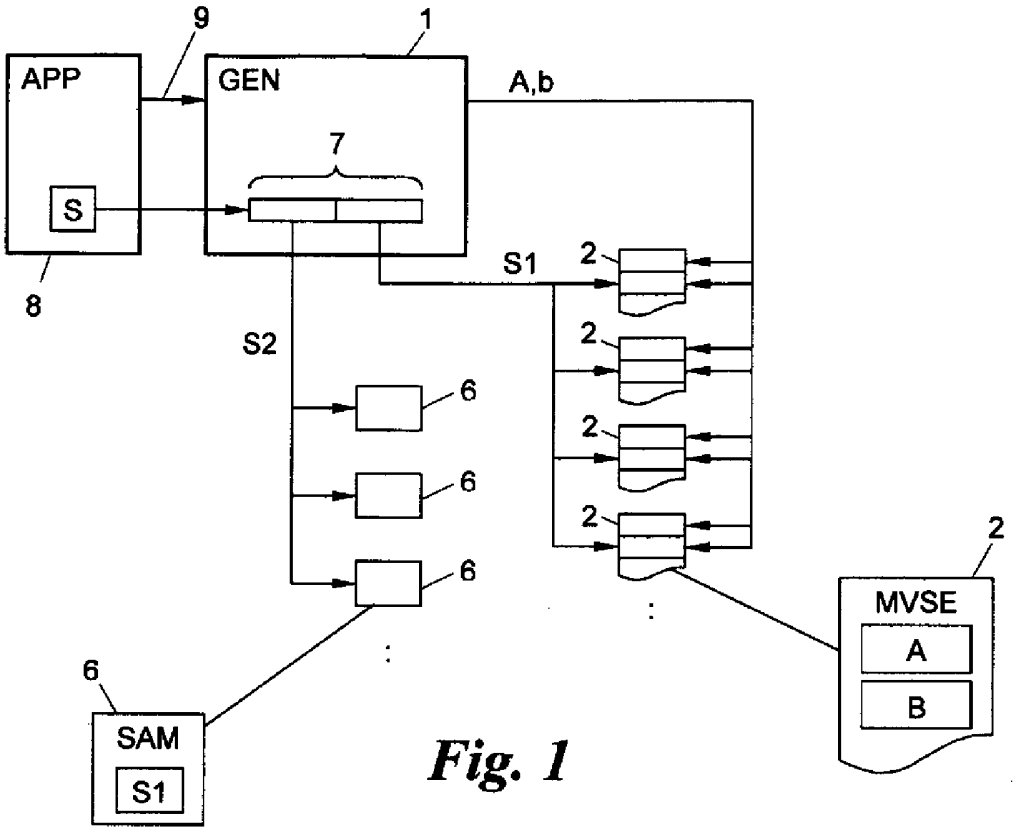
9
1
APP
GEN
A,b
7
S
8
S1
2
S2
6
MVSE
A
B
SAM
S1

Fig. 1

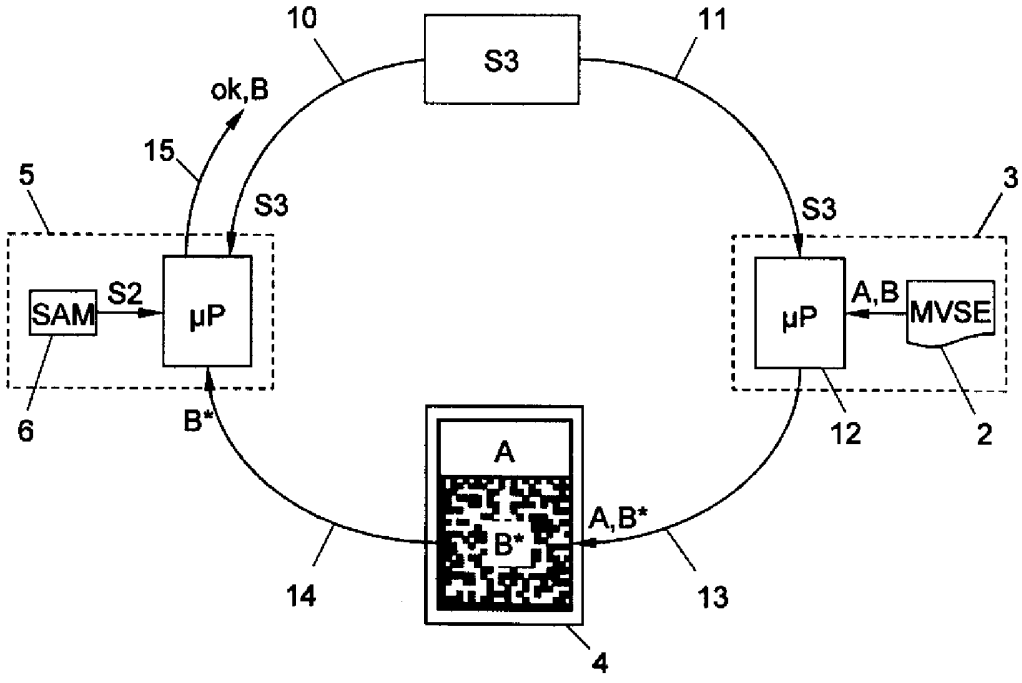
10
S3
11
ok,B
15
5
S3
S3
3
SAM
S2
µP
µP
A,B
MVSE
6
B*
12
2
A
B*
A,B*
14
13
4

Fig.2