19

Secure Billing – Incontestable Charging

S. Pütz
University of Siegen, Hölderlinstraße 3, 57076 Siegen, Germany
Department for Electrical Engineering and Informatics
Tel.: (0271) 740 - 2623, Fax: (0271) 740 - 2536
e-mail: puetz@nue.et-inf.uni-siegen.de

Abstract

To be able to recognize fraud as well as faults in the charging process and thus to avoid incorrect bills, this paper presents a verifiable method of charge accounting by introducing charge tokens which mark beginning and end of chargeable service utilisations. Ingenious and applicable charging quantities and types, different methods of charge accounting as well as the handling of charge tokens are discussed. To avoid injustices on charges resulting from forced disconnections intermediate service tokens will bound the risk of having to bear costs in case of a not correctly signalized service end to a calculable limit. Furthermore, the different confidential relationships between service user and provider existing for each charging variant are described, the requirements on the charge tokens are defined and their conversion into protocol data units is demonstrated.

Keywords

Secure billing, incontestable charging, security techniques, non-repudiation, digital signatures, asymmetric cryptographic mechanisms, timestamps, confidential relationship

1 INTRODUCTION

Modern communication systems should be capable of providing a reliable and comfortable method of charging the costs of utilization. However, up to now the service user has not been involved in the process of recording and generating the usage charges. For this reason he is not in the position of verifying the charges invoiced to him. If any charge units are unjustifiably booked to his account, he can neither reconstruct this nor can he prove that the erroneously billed units are not due to the use of his subscriber access. The charging information lacks one characteristic which indicates in a verifiable form that these specific charge data were caused by a certain user and could have been caused only by him alone.

P. Horster (ed.), *Communications and Multimedia Security II*

To be able to recognize faults in the charging process and thus to avoid erroneous bills, this paper presents a verifiable and reconstructible method of charge accounting. This method protects the user of a service from being unjustifiably charged by the service provider. On the other hand, the user cannot deny towards the service provider that he has utilized the service for which he was billed.

The basis of the verifiable charge account consists in the fact that the user is involved into charge generation process. Therefore a method is basically required which, similar to delivery notes and receipts in freight traffic and mail-order trade, verifiably proves the utilization of a service as well as its payment or remunification.

This basic function is taken over by charge tokens which are structured according to the non-repudiation mechanism [ISO_10181, ISO_13888-1 and -3], based on the use of digital signatures [ISO_9796, ISO_14888, Rula_93] and supported by asymmetric cryptographic algorithms. In the sense of charge accounting, the charge records serve as non-repudiation of origin tokens. They link the action or event indicated in the NRO and the originator in such a way that the originator cannot deny his originatorship. On the other hand the originator is able to prove his originatorship against any third party. In the accounting records the originator certifies that he has provided or utilized a chargeable service.

Should, nevertheless, a dispute arise between service provider and user about the accounting of charges, it can be settled with the aid of the charging tokens. In case of doubt, a trusted third party is to be contacted for this purpose.

Since the utilization period corresponds to the accounting-relevant characteristic of a telephone call, it suggests itself to generate the charging units for telephone calls on a time-dependent basis. The accounting quantity is formed by the time interval between beginning and end of service utilization. In the event of data transmission like fax or file transfer (also over mobiles), it appears to be reasonable to take the transmitted data volume as accounting basis. As charging quantity, use can be made of the actually transmitted net message length, that means the length of the layer-4 protocol data units [ISO_7498]. Further services such as the Short Message Service (SMS) can be regarded as *one-time services* and be billed with a flat rate per service rendered.

2 CHARGING PRINCIPLES

2.1 Charging quantities

As charging basis various basic quantities come into consideration. According to the type of service, it is for instance possible to distinguish between time-, volume- or event-dependent charging quantities (CQ). In the text below the usage duration (UD) of a chargeable service utilization is bounded by start-of-service (SS) and end-of-service (ES).

2.1.1 Time-dependent charging

As time-dependent charging quantity use is made of the actual time of service utilization. If a charge token, marked as start-of-service token (SST), describes the usage beginning (SS) of a chargeable service in a trustworthy way and if, additionally, its usage end (ES) is indicated verifiably by an end-of-service token (EST), these records allow the usage duration (UD) to be calculated and a reconstructible bill can be issued [Pütz_95]. Charge registration is based on the charging duration (CD) which normally coincides with the usage duration (UD).

2.1.2 Volume-dependent charging

As volume-dependent charging quantity the net message length finds application. If the really transmitted message or usage volume (UV) of a chargeable service is reliably described by the charging records, i.e. start-of-service tokens (SST) and end-of-service tokens (EST), these records permit the calculation of the charging volume (CV) and a reconstructible bill can be prepared. Charge registration thus is based on the charging volume (CV) which usually corresponds with the usage volume (UV).

2.1.3 Event-dependent charging

Individual services such as SMS can be regarded as *one-time services* and be charged at a flat rate per service rendered. If these single services are described unambiguously and reconstructibly by service identifiers, a verifiable bill can be made out on the basis of these records. Charge registration thus is event-oriented.

2.2 Types of charging

In principle, charging mechanisms can be subdivided into two categories: flat-rate and usage-based charging [FJKP_95]. Combinations of both types are possible, but in that case the properties of the two basic mechanisms have to be taken into consideration.

2.2.1 Flat rate charging

Flat rate charging signifies that the service user is not charged with single services, but that a lump sum is debited to all users (for a defined period of utilization). During this period the user may utlize the services offered as often as he wishes.

2.2 2 Individual usage- and performance-based charging

The opposite method to flat rate charging is the usage- or performance-based type of charging. The user is charged with the services actually rendered to him. Usage- or performance-based charging can be executed in two ways: by pre- or by post-acknowledgement.

2.2.2.1 Pre-acknowledgement

Pre-acknowledgement signifies that the user acknowledges a service offered in advance that means *before* he makes use of it. A charge record is generated prior to the service utilization and obligates the user to pay for it accordingly. Accounting of the records can be made as outlined in paragraph 2.2.3.

2.2.2.2 Post-acknowledgement

An alternative to the pre-acknowledgement is the subsequent acknowledgement of the services rendered. The user is *after* service utilization debited with the services actually used (possibly accumulated). For this purpose a charge token is issued subsequently to the service utilization and the user commits himself to settle it. Accounting of these records can be effected in accordance with paragraph 2.2.3.

2.2.3 Payment transactions

Accounting of the charge tokens can be carried out by setting off the amounts due with a credit balance of the service user, that means with an amount paid in advance, or subsequently by payment of a bill. The settlement can, of course, also be made with credit cards, electronic cash or other untraceable payment systems.

2.2.4 Discussion of the types of charging

In the flat rate charging variant the service provider is compensated with a predetermined amount for all services which the user utilizes during a fixed period. Sporadic users pay the same as permanent users. The advantage of this method is its simplicity because the charging data hardly cause any signalling traffic inside the networks [FJKP_95]. It may, however, result in great injustice among the service users. More justice will be reached by an individual usage- and performance-based charging variant, where the user pays only for those services which he has actually made use of.

However, there is no guarantee that all services are duly completed. Disconnections or interruptions of calls which may be caused by different events have to be taken into account. They pose some problems for the individual usage- and performance-based charging variant. Basically, it applies in this case that a distinction has to be made between system-related (random) and forced or mandatory disconnections. Whereas system-related call disconnections cannot be completely avoided, it is not unlikely that abortions by the service user or provider can intentionally manipulate charge registration. For example, an interruption of the power supply of a mobile terminates an instantaneously existing connection before the cleardown of the connection and thus the end of the service utilization were correctly signalized.

The difference between the pre-acknowledgement (see paragraph 2.2.2.1) and the post-acknowledgement (see paragraph 2.2.2.2) will here be illustrated by the example of the public telephone service of *Deutsche Telekom*. After a call between two users has been switched through, the account of the calling party is debited with a charging unit. This corresponds in principle to the pre-acknowledgement because the charges are booked irrespectively of the complete rendering of the service. Contrary to this, a booking of charging units after the complete provision of a service corresponds to the post-acknowledgement.

If services are remunerated against pre-acknowledgement, the user pays, in case of a disconnection, the full amount for a possibly not completely rendered service. On the other hand, in case of post-acknowledgement, the service provider can – as a result of a call interruption – not bill a service which he has not completely rendered.

Depending on the types of charging, the risk of having to bear the costs in the event of a disconnection rests with one of the two parties, either with the service user or provider. To make this risk calculable, is one objective of the billing method proposed in paragraph 3.

3 PROPOSAL FOR A VERIFIABLE BILLING METHOD

The proposal presented below is a combination of the two acknowledgement mechanisms described in paragraph 2.2.2.

On the assumption of regular call set-up and cleardown operations, it is sufficient to describe the utilization of a service by its beginning and its end. If, however, the disconnection of a call leads to the premature end of utilization, the end is marked in a non-reconstructible

form. Disconnection or interruption of a call – whether at random (noise, diffraction loss, handover) or forced (operator errors, attempts of fraud) – cannot be avoided in communication systems, particularly in mobile radio system. In order to guarantee, nevertheless, a safe and reliable charge accounting process, the total usage time or the total usage volume are subdivided into usage sections. These usage sections can be described by intermediate service tokens ($IST_{i,j}$). The index i indicates the association of the intermediate service token $IST_{i,j}$ with the service utilization i, the beginning of which is described by SST_i. j represents a continuous numbering of the intermediate service tokens $IST_{i,j}$ of service utilization i.

A further advantage of the intermediate service tokens consists in limiting the charge amounts to a maximum charge per intermediate service token. This limitation prevents, for instance, that charge amounts are summed up to values which exceed this upper limit and then to evade the payment obligation by a forced abortion of the call.

The following legend gives a short overview of the abbreviations used.

UD_i: Usage duration of service utilization i in time units
UV_i: Usage volume of service utilization i in volume units

CD_i: Charging duration of service utilization i in time units
CV_i: Charging volume of service utilization i in volume units

CQ_i: Charging quantity of service utilization i in [sec, bits or per event]

SS_i: Start-of-service utilization i with respect to system time
ES_i: End-of-service utilization i with respect to SS_i

SST_i: Start-of-service token describing start-of-service utilization i (SS_i)
EST_i: End-of-service token describing end-of-service utilization i (ES_i)
$IST_{i,j}$: jth intermediate service token indicating the intermediate acknowledgement of service utilization i, j = 1, 2, 3, ...

The charge tokens SST_i, EST_i and $IST_{i,j}$ are formed by charging records.

MS: Maximum size of an intermediate service token in time or volume units

As an example of the usage-dependent type of charging in regular operation, Fig. 3.1 shows the registration of the usage duration UD_i and the charging duration CD_i for the service utilization with index i = 1 and the regular and undisturbed case of charging.

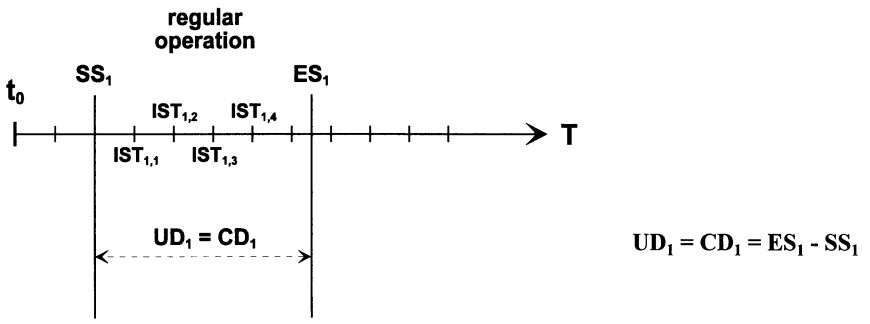

Figure 3.1: Record of charging duration for "regular operation"

Fig. 3.1 can be changed into an example for the volume-dependent charging quantity by replacing the time axis by a volume-dependent quantity like the message length expressed in bits. For the usage volume UV_i and the charging volume CV_i there holds then accordingly $UV_1 = CV_1 = ES_1 - SS_1$.

With each new intermediate service token the previous one loses its significance. If the service utilization i in regular operation is ended with EST_i, in addition to all further $IST_{i,j}$ the last $IST_{i,j}$ of this service utilization i becomes meaningless and can be discarded. If, however, a call interruption leads to the premature termination of the service utilization, there exists the last charge record from the intermediate service token $IST_{i,j}$ with j = j_max. The value of the charging quantity CQ_i, that means the charging duration CD_i or the charging volume CV_i, results then from the difference of IST_{i,j_max} and SS_i. The higher the resolution of the intermediate service tokens, i.e. more frequently intermediate service tokens are generated per time or volume unit, the more precisely the usage end due to a call interruption can be described.

As an example of charge accounting in the event of call interruption, Fig. 3.2 shows the record of the usage duration UD_i and the charging duration CD_i for the service utilization with the index i = 2. The usage end ES_2 marks the instant of the call interruption. The usage duration thus results from ES_2 and SS_2 as $UD_2 = ES_2 - SS_2$. As last intermediate service token $IST_{i,j}$ is generated with j = j_max = 4. Therefrom we obtain the charging duration $CD_2 = IST_{2,4} - SS_2$. The difference between the usage duration UD_2 and the charging duration CD_2 results as absolute value $| UD_2 - CD_2 | = ES_2 - IST_{2,4}$.

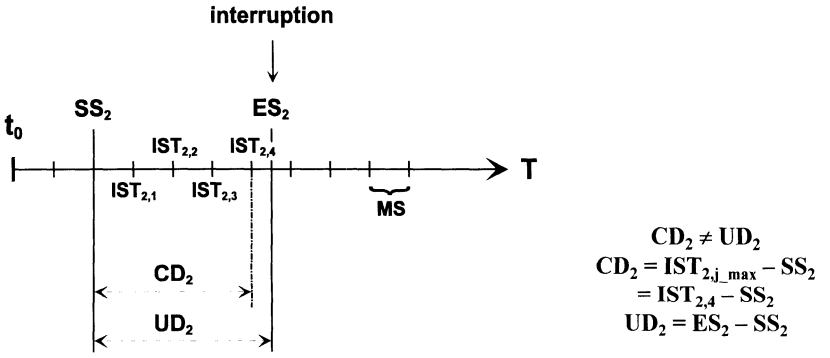

Figure 3.2: Record of charging duration "interruption – variant I"

Fig. 3.2 can be converted into an example for the volume-dependent charging quantity by replacing the time axis by a volume-dependent quantity like the message length in bits. For the usage volume UV_i and the charging volume CV_i there holds then accordingly $UV_2 = ES_2 - SS_2$ and $CV_2 = IST_{2,4} - SS_2$ respectively as well as $| UV_2 - CV_2 | = ES_2 - IST_{2,4}$.

If the charges after a call interruption are calculated in the previously described form, the service provider bears the costs for the difference between the real usage duration UD_i (or the usage volume UV_i) and the charging duration CD_i (or the charging volume CV_i). If all $IST_{i,j}$ in the respective unit have a maximum size MS, so that for the utilization sections described by the intermediate service tokens $IST_{i,j}$ there holds $IST_{i,j+1} \leq IST_{i,j} + MS$, there exists a further variant of charge accounting, indicated as variant II.

In this variant CD_i (or CV_i) is obtained from the difference of $IST_{i,j}$ + MS with j = j_max and SS_i. This means that the service user is debited additionally to the charges up to the intermediate service token IST_{i,j_max} also with the charges for the maximum size of an intermediate service token. For a fixed size of the intermediate service tokens this variant describes the charging method which is at present applied in the telephone service. Here started charge units are considered to be used up even if they were not fully utilized. Charging thus takes place per started charge unit.

Fig. 3.3 depicts an example of recording the usage duration UD_i and the charging duration CD_i of the service with index i = 3 as a result of a interruption according to variant II. The usage end SE_3 again marks the instant of the call interruption. The usage duration UD_3 is thus derived from SE_3 and SS_3 to $UD_3 = ES_3 - SS_3$. As last intermediate service token $IST_{3,j}$ with j = j_max = 4 is generated. Therefore, the charging duration CD_3 results in $CD_3 = IST_{3,4} + MS - SS_3$. The difference between the usage duration UD_3 and the charging duration CD_3 results as absolute value $|UD_3 - CD_3| = IST_{3,4} + MS - ES_3$.

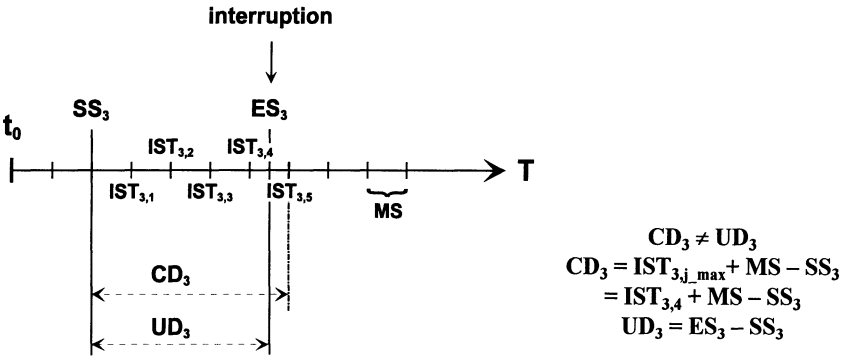

Figure 3.3: Record of charging duration "interruption – variant II"

Fig. 3.3 can be changed into an example for the volume-dependent charging quantity by replacing the time axis by a volume-dependent quantity like the message length expressed in bits. For the usage volume UV_i and the charging volume CV_i there holds then analogously $UV_3 = ES - SS_3$ and $CV_3 = IST_{3,4} + MS - SS_3$ respectively as well as $|UV_3 - CV_3| = IST_{3,4} + MS - ES_3$.

Both variants lead to injustices because – irrespective of the fact who has caused the interruption of the call – always the same party (service user or provider) has to bear the additional charges. The amount of these additional charges corresponds to the indicated difference between usage duration and charging duration or between usage volume and charging volume. The variant I according to Fig. 3.2 is to the disadvantage of the service provider, variant II according to Fig. 3.3 to that of the service user.

Therefore, a further variant provides for an application the causation principle. The charges resulting from the difference between the actual usage duration UD_i and the charging duration CD_i are debited to the party that has caused the call interruption. To identify the responsible side, it is necessary to detect the cause (and thus the causing party) in a trustworthy way. This idea will not be pursued here any further.

3.1 Risk minimization and protection against fraud by means of intermediate acknowledgements

In regular operation (see Fig. 3.1) a safe and reliable charging procedure is ensured by the application of start-of-service and end-of-service tokens. Digital signatures and the non-repudiation mechanism provide protection against fraud and manipulation. But it is also desirable to prevent any attempt of fraud in case of regular operation if that is interfered with intentionally or by influences of the transmission channel (e.g. fading, handover). For this reason we will deal in the following with intermediate service tokens in variant I and II in the event of a interruption.

Depending on the variant applied, there is a difference in the meaning of intermediate service tokens $IST_{i,j}$. Variant I in Fig. 3.2 provides that intermediate service tokens describe services which have already been utilized. Accordingly these acknowledgements have a kind of invoice character. In variant II of Fig. 3.3, on the other hand, intermediate service tokens are issued in advance, that is prior to the utilization of a service described by a special intermediate service token. In that case the acknowledgements have the character of pre-payment or advance remuneration (example: public telephone service).

Generally the introduction of intermediate service tokens reduces the risk of fraud for both parties. It can, however, not be excluded that the service user and the service provider, respectively refuse the intermediate service token and the service already acknowledged. But this risk will be calculable by a sufficiently small (equidistant) division of the intermediate service tokens. Nevertheless, it becomes apparent that, depending on the variant chosen, a unilateral confidential relationship must exist between service user and service provider. In variant I the service provider trusts in the correct issuing of the intermediate service tokens by the service user. On the other hand, in variant II the service user expects that the service provider actually renders the service already acknowledged by the service user.

Since attempts of fraud by the service user can be stored and evaluated by the service provider, the overall risk of the service provider is smaller than that of the service user. As a consequence, it is possible to withdraw the service user his network access rights and by that deny him a further utilization of the service. If the service user notices a fraud attempt by the service provider, he will discontinue his service utilization and file a complaint at the competent authority.

3.2 Handling of intermediate service tokens

After having treated risk minimization by means of intermediate service tokens in paragraph 3.1, we will now turn to their handling. Since intermediate service tokens represent a unilateral acknowledgement of a service issued by the service user for the service provider, an unprotected, non-acknowledged transmission of the intermediate service tokens to the service provider is sufficient.

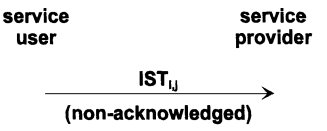

Fig. 3.4: Non-acknowledged intermediate service token

Fig. 3.4 shows the non-acknowledged transmission of a intermediate service token to the service provider. In contrast to this, Fig. 3.5 indicates that the service provider confirms the intermediate service token with an acknowledgement.

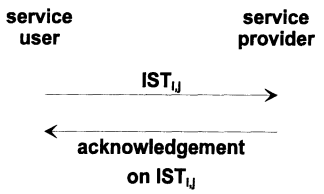

Fig. 3.5: Acknowledged intermediate service token

Whereas a service according to the non-acknowledged method can be interrupted as a result of a loss of data or errors during the transmission of an intermediate service token, the service user, when using the acknowledged procedure, has the certainty that his intermediate service token has reached the service provider and has been accepted by him. This means, however, a considerable increase in protocol-efforts due to the additional acknowledgement.

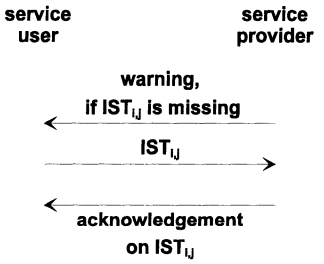

Fig. 3.6: Warning in the event of non-arriving of an intermediate service token

Fig. 3.6. represents a variant of the two methods mentioned before. Here the service provider has the possibility to send a reminder when no intermediate service token arrives within a predefined time-interval. In that case the service user will be warned that the undisturbed continuation of the service is at risk. The repetition of an intermediate service token can for instance help to avoid transmission errors. IST will be confirmed by a acknowledgement.

Fig. 3.7 depicts a flow chart for the handling of intermediate service tokens. At first the service user sends non-acknowledged intermediate service tokens to the service provider. When an intermediate service token is due, he receives a reminder by the service provider. Now the user has several possibilities. He can dispatch the overdue service token late. If the intermediate service token has got lost, he can send it off once again. The third possibility consists in the dispatch of an updated or the following intermediate service token because with each new intermediate service token each previous one will become irrelevant. Thereafter he sends again, without being requested, non-acknowledged intermediate service tokens to the service provider.

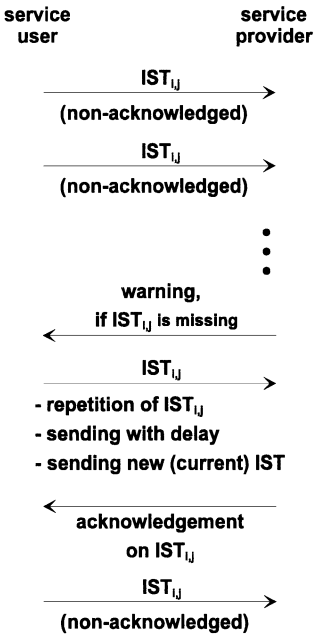

Fig. 3.7: Flow chart

3.3 Requirements on charge tokens

3.3.1 Start-of-service token

The token on the beginning of service utilization SST_i describes the start of a chargeable service SS_i which the service provider is to render to the service user. Therefore the token must contain the unambiguous identity of service provider and user, type and volume of the chargeable service and at least, as non-recurrence verification [Pütz_95], the time when the service has started. The necessity of describing type and volume of the service depends on the underlying charging quantity. Flat rate services require the precise specification of the type of service, whereas usage- and performance-based charging quantities necessitate a description of the charging quantity and of the maximum size of the following intermediate service tokens. An unambiguous identification of the token facilitates the allocation of possibly following intermediate service tokens and of the end-of-service token to this start-of-service token and thus also to the service concerned. In order to prevent manipulations, the integrity and authenticity of these data are required. Just like the service user the service provider must acknowledge all data included in the start-of-service token in a reconstructible form as the beginning of the chargeable service (e.g. by double signature).

The requirements to be satisfied by the start-of-service token are summarized below:

- Unambiguous identification of service user and provider
- Type and volume of the service, maximum size of an intermediate service token
- Timestamp at which the service has started

- Identification allowing a simple allocation of following intermediate service tokens or the end-of-service token
  Alternative: inclusion of a hash value calculated on the total start-of-service token as identification into the following charge tokens
- Integrity and authenticity
- Proof by service provider and service user that the charge-relevant starting value of the charging quantity is accepted as the actual starting value.

3.3.2 Intermediate service token

Intermediate service tokens describe a (partial-) service which the service provider renders to the service user. Therefore, the identities of service user and provider as well as the extent of the (partial-) service must clearly be indicated in the intermediate service token. If an intermediate service token refers to a start-of-service token SST_i, it is sufficient to establish, instead of the identities and the extent of the service, an unambiguous relationship between the SST_i and the intermediate service token (random number, hash value). See paragraph 3.3.1. A sequence number j characterizes all intermediate service tokens of the same service with the index i. Integrity and authenticity of the intermediate service token must be guaranteed in order to protect against manipulations.

The requirements placed on intermediate service tokens are summarized below:

- Unambiguous identification of service user and provider
  or (alternatively) unambiguous relationship to start-of-service token
- Unambiguous identification of (partial-) service volume (alternatively)
- Consecutive numbering of all intermediate service tokens of the same service i
- Integrity and authenticity

3.3.3 End-of-service token

The end-of-service token describes the completion of a service which the service provider has rendered to the service user. Therefore, the identities of service user and provider must clearly be indicated by the end-of-service token. As an alternative, an unambiguous relation (see paragraph 3.3.2) can be established between the start-of-service and end-of-service tokens. To be able to calculate the service volume, the final value of the charge quantity is described. From it and from the corresponding start-of-service value, which can be taken from the start-of-service token, it is possible to determine the usage duration or usage volume. In order to protect the end-of-service token against manipulation, its integrity and authenticity must be guaranteed. Moreover, it has to be ensured that in addition to the service user also the service provider recognizes all data with which the end-of-service token describes the completion of the chargeable service in a reconstructible form (e.g. by double signature).

The requirements to be satisfied by the end-of-service token are summarized below:

- Unambiguous identification of service user and provider
  or (alternatively) unambiguous relationship to start-of-service token
- Unambiguous identification of total service volume or final end-of-service value
- Integrity and authenticity
- Proof by service provider and service user that charge-relevant final value of the charge quantity is accepted as the actual final value.

4 CHARGING TOKENS AS PROTOCOL DATA UNITS

The following legend comprises all abbreviations used in the protocol data units of the charging tokens. The notation complies with the ISO-nomenclature; see e.g. [ISO_9798].

s:	Digital signature giving message recovery
S_x:	Private key of an asymmetric key pair of X
H(*m*):	Hash function, that indicates a cryptographic check value calculated on message *m*
***u* || *v* || ... :**	Concatenation of two or more data units to message $m = u \,||\, v \,||\, ...$
SP:	Identity of service provider
USER:	Identity of service user
$ID_{SERVICE}$:	Service identifier
$ID_{PARTSERVICE}$:	Identifier of partial service
$ID_{TOTALSERVICE}$:	Extent of total service
ID_{MS}:	Maximum size of intermediate service token
	$ID_{PARTSERVICE}$, $ID_{TOTALSERVICE}$, and ID_{MS} can – depending on the charging quantity – represent a fixed value, a meter reading or a timestamp.
ID_{SST}:	Identifier of start-of-service token
ID_{EST}:	Identifier of end-of-service token
ID_{IST}:	Identifier of intermediate service token
STS:	Secure timestamp
RND:	(Pseudo-) random number
SEQ:	Sequence number

4.1 Start-of-service token

The SST takes the following form:

$$sS_{SP}((...) \,||\, sS_{USER}(...)) \quad \text{with } (...) = ID_{SST} \,||\, USER \,||\, SP \,||\, ID_{SERVICE} \,||\, ID_{MS} \,||\, STS \,||\, RND$$

sS_{SP} (sS_{USER} (...)) represents a double signature of the internal data package (...). This double signature ensures that both service provider and service user have verifiably accepted the internal data package. The signatures should therefore be preceded by a check of the data to be signed. The same applies to the end-of-service token in paragraph 4.3.

If a hash value on the start-of-service token is used in the following intermediate service tokens and in the end-of-service token as unambiguous reference, the random number RND is omitted in the start-of-service token which then takes the following form:

$$sS_{SP}((...) \,||\, sS_{USER}(...)) \quad \text{with } (...) = ID_{SST} \,||\, USER \,||\, SP \,||\, ID_{SERVICE} \,||\, ID_{MS} \,||\, STS$$

4.2 Intermediate service token

The IST takes the following form:

$$sS_{USER}(...) \quad \text{with } (...) = ID_{IST} \,||\, RND \,||\, ID_{PARTSERVICE} \,||\, SEQ$$

Instead of the random number RND reused from the start-of-service token, it is possible to use in its place a hash value $H(NB_i)$ calculated on the corresponding start-of-service token. Consequently, the intermediate service token has the following form:

$$sS_{USER}(...) \qquad \text{with } (...) = ID_{IST} \| H(NB_i) \| ID_{PARTSERVICE} \| SEQ$$

4.3 End-of-service token

The EST takes the following form:

$$sS_{SP}((...) \| sS_{USER}(...)) \qquad \text{with } (...) = ID_{EST} \| RND \| ID_{TOTALSERVICE}$$

Alternatively to the reused random number RND from the start-of-service token, it is possible to use in its place a hash value $H(NB_i)$ calculated on the corresponding start-of-service token. Thus the end-of-service token has the following form:

$$sS_{SP}((...) \| sS_{USER}(...)) \qquad \text{with } (...) = ID_{EST} \| H(NB_i) \| ID_{TOTALSERVICE}$$

4.4 Classification of service identifier

The classification of service identifier can be seen in Table 4.1. $ID_{SERVICE}$ marks the charging quantity the bill is based upon. If the charging process is carried out time- or volume-dependent $ID_{PARTSERVICE}$ and $ID_{TOTALSERVICE}$ contain the extent of service up to that point. The starting time of the service is described by the timestamp in the start-of-service token.

Table 4.1: ID-Classification

charging quantities	$ID_{SERVICE}$	$ID_{PARTSERVICE}$	$ID_{TOTALSERVICE}$
time-dependent	ID_{TIME}	accumulated usage time	total usage time
volume-dependent	ID_{VOLUME}	accumulated usage volume	total usage volume
event-dependent	ID_{EVENT}	—	—

5 SUMMARY

Various charging quantities and different charging mechanisms were presented in this contribution. Accounting of flat rate services is guaranteed by special charging tokens. Thanks to the introduction of start-of-service and end-of-service tokens, it is possible to document usage- and performance-dependent services in a reconstructible form. Intermediate service tokens divide the charging period or the charging volume into maximum intervals and thus minimize the risk that bills are manipulated, e.g. by forced disconnections. In conclusion, the requirements which have to be satisfied by the three kinds of charge tokens, the start-of-service and end-of-service tokens as well as the intermediate service tokens are defined and their construction as protocol data units is demonstrated.

6 REFERENCES

FJKP_95 Federrath, Hannes; Jerichow, Anja; Kesdogan, Dogan; Pfitzmann, Andreas: *Technischer Datenschutz in öffentlichen Mobilkommunikationsnetzen.* Wissenschaftliche Zeitschrift der TU Dresden, 1995.

ISO_7498 International Organisation for Standardization (ISO): *Open Systems Interconnection: Basic Reference Model.* International Standard ISO 7498, 1983.

ISO_9796 International Organisation for Standardization (ISO): *Information technology - Security techniques - Digital signature scheme giving message recovery.* ISO / IEC 9796, 1991.

ISO_9798 International Organisation for Standardization (ISO): *Entity authentication mechanisms - Part 3: Entity authentication using a public - key algorithm.* Draft International Standard ISO DIS 9798 - 3, 1992.

ISO_10181 International Organisation for Standardization (ISO): *Information technology - Open Systems Interconnection - Security frameworks in Open Systems - Part 4: Non - repudiation.* ISO / IEC DIS 10181 - 4.2, 1995.

ISO_13888-1 International Organisation for Standardization (ISO): *Information technology - Security techniques - Non-repudiation - Part 1: General Model.* 2nd ISO / IEC CD 13888 - 1, 1995.

ISO_13888-3 International Organisation for Standardization (ISO): *Information technology - Security techniques - Non-repudiation - Part 3: Using asymmetric techniques.* ISO / IEC CD 13888 - 3, 1995.

ISO_14888 International Organisation for Standardization (ISO): *Information technology - Security techniques - Digital signatures with appendix.* ISO / IEC CD 14888.

Rula_93 Ruland, Christoph: *Informationssicherheit in Datennetzen.* DataCom - Verlag, Bergheim, 1993.

Pütz_95 Pütz, Stefan: *Neue Lösungsansätze für Authentikation in künftigen Mobilfunksystemen.* 2. ITG - Fachtagung „Mobile Kommunikation '95". ITG - Fachbericht 135, vde - Verlag GmbH, Berlin, Offenbach, 1995, S. 411 - 422, Hrsg.: Walke, B.

7 BIOGRAPHY

Stefan Pütz received the Dipl.-Ing. in electrical engineering from the University of Siegen in 1994. Since that time he works at the Institute for Data- and Telecommunications and develops security systems for future open and heterogeneous mobile radio systems. A verifiable and mutual authentication between participants and system components will be guaranteed by applying the non-repudiation mechanisms to mutual agreements.