3GPP/PCG Meeting#2
Sophia Antipolis,
6-7 July 1999

3GPP/PCG#2(99)6
1 July 1999
page 1 of 17

Source: **TSG SA**

Title: **Criteria for Cryptographic Algorithm Design Process**

Agenda item: **8**

Document for:

Decision	
Discussion	
Information	X

The attached technical report was prepared by TSG SA WG3 and was approved by TSG SA during their meeting in Miami on 21-23 June 1999.

3G TR 33.901 V1.0.0 (1999-06)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Criteria for cryptographic algorithm design process
3G TS 33.901 V 1.0.0

Reference

DTS/TSGS-________

Keywords

Security, Algorithms, Design, Criteria

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This document has been drafted by 3GPP TSG-SA WG 3, i.e., the Workgroup devoted to "Security" issues, within the Technical Specification Group devoted to "System Aspects".

1 Scope

This report discusses the possibilities for acquisition of the cryptographic algorithms that has to be standardised in UMTS. The focus is on the encryption function used in the data confidentiality mechanism and the message authentication function used in the signalling data integrity mechanism.

First certain aspects of the process and desired results for an algorithm specification and their pro's and cons will be given. These aspects will include the possible design strategies, the evaluation strategies, the possibilities for distribution of the algorithms and the options for the liability and responsibility for the algorithm.

Then a number of the most realistic scenarios for the algorithm specification will be presented. These scenarios will be used as a basis to make a final choice for the specification process for cryptographic algorithms in third generation mobile systems. Finally, a preferred procedure will be described.

2 References

[1] 3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

3 Introduction

3.1 Algorithms, export control and flexibility

In the "3G Security: Objectives and Principles" document [1], it is stated that strength of the encryption confidentiality service will be greater in UMTS than that used in second generation systems (the strength is a combination of key length and algorithm design). It is decided that a new confidentiality algorithm is needed. An algorithm for message integrity services (MAC) is also required.

In practice the application of encryption algorithms is limited by export controls.

Recently a group of 33 major Industrial countries joint in the so-called Wassenaar Arrangement agreed to set the limit the key length for export of encryption capable algorithms to 56 bits. Encryption algorithms with a longer key length will be subject to export controls.

The "3G Security: Threats and Requirements" document [2] states that the security features standardised should be compatible with world-wide availability. This requirement mainly concerns the confidentiality algorithm. MAC algorithms are usually not subject to export control. In [2] is also stated that it should be possible to enhance and extend the UMTS security features and mechanisms as required by new threats and services.

It can be expected that export control rules will vary over time. Also the requirements on the strength of cryptographic mechanisms might vary with time and could depend on the geographic environment.

Therefore the security mechanisms for UMTS should cater for flexibility. In this paper we assume that the above flexibility can in the first place be achieved via key length variations. If an option with several different algorithms is used, this will only mean that more resources have to be assigned for evaluation and if applicable for the design. See discussion below.

3.2 Design and evaluation methods

Each algorithm needed can be acquired by selecting it from available off the shelf algorithms, inviting submissions or commissioning of a special design group for its development. These three methods are applicable for *secret algorithms*, i.e. algorithms that are intended to be kept secret, as well as for *open algorithms*, i.e. algorithms that are published. The choice between these methods constitutes the *design strategy*.

All algorithms have to be evaluated regarding strength. Their stated level of security should correspond to the actual security offered. It is important that the algorithms can be trusted to provide the level of security they claim to offer. This trust could be created during the design and a subsequent evaluation phase.

The available methods for evaluation are either to rely on voluntary efforts or to commission a group of experts. The evaluators would of course review any existing evaluation reports and do their own analysis. The method used is called the *evaluation strategy*.

The design strategy, the evaluation strategy and the available proof/documentation will of course influence the level of trust of the end users in an algorithm.

3.3 Responsibility for algorithms.

In the end, someone has to take responsibility for the algorithms. Which party e.g. is liable if the algorithm is broken en financial losses occur.

In case of a commissioned design the responsibilities are more or less clear. In principle the person/organisation which commissions the design is responsible, but some of the responsibility might, e.g. by contract, be transferred by the party, which takes on the task to design the algorithm.

In case of an open call for algorithms the responsibility for the algorithm is less clear. It is probably not realistic to make responsibility part of the call (i.e. if you are submitting an algorithm and it will be used then you are liable if it is broken). So the responsibility lies with the party selecting the algorithm. But it is not clear if this selecting party is able to take on any responsibility. This will depend on the process, which is applied.

An option in both cases might be to make the algorithm available (distributing, publishing) without taking any responsibility.

3.4 ETSI algorithms and procedures

ETSI has over the years developed its own way to deal with the design of standard algorithms. The technical work in ETSI is mainly done by Technical Committees (TC’s), working on a specific area of telecommunications, and ETSI Projects (EP’s), working on a specific telecommunications system. Also there are a few special committees working on a very specific subjects. The specification of security standards for a specific telecommunications area or system is in principle carried out by the responsible TC or EP. For general security issues and support ETSI established a Technical Committee, TC Security. For the design and specification of algorithms a Special Committee was installed: the Security Algorithm Group of Expert (SAGE). Unlike other TC’s or EP’s, SAGE is a closed group with an appointed membership.

The outline procedure for the design of cryptographic algorithms for ETSI standards currently is as follows. First an ETSI TC or EP establishes the need for a standard cryptographic algorithm. Then the TC/EP drafts a document specifying the requirements for this algorithm. These requirements usually are directed at issues such as use of the algorithm and its specification, implementation complexity, performance, resilience, exportability, and management of the algorithm and its specification. The document also specifies if the algorithm should be published or kept confidential (and distributed under a non-disclosure agreement). If needed, TC Security assists the responsible committee to draft the algorithm requirements.

In the next phase ETSI SAGE designs and specifies the algorithm according to the requirements. The algorithm is then delivered to the algorithm custodian (in most cases this is ETSI) which takes care of the distribution of the algorithm to the intended users.

SAGE produces a report for the committee, which outlines the work done the results achieved and the rules for management of the algorithm.

From this point on the algorithm custodian starts distributing the algorithm to those requesting for it. In Annex A an overview of standard ETSI cryptographic algorithms is given.

4 Requirements, constraints, options and consequences

4.1 Security architecture and mechanisms

High level requirements on the system might influence the feasibility of a chosen design strategy. For example, if the system will contain many algorithms in the authentication procedures, lack of resources for design and evaluation might introduce unacceptable delays. *In this paper we assume that only a MAC algorithm and an encryption algorithm should be acquired.*

Assumptions:

4.2 Suitable / Tailored for use algorithms

Basic requirements for the confidentiality service is that it should be possible to encrypt 2 MB/s and have fast context switching, i.e. that switching between keys and contexts for different users should be fast. The MAC calculations should be as fast as possible. Both functions should have efficient hardware and software implementations. The main focus is on hardware implementation of the confidentiality algorithm. *Usually a special purpose design will perform better than a general solution.* For MAC the advantage is not so obvious.

Assumptions:

A special purpose design will perform better than a general solution. For MAC the advantage is not so obvious

4.3 Open and secret algorithms

The protection offered by an algorithm should always be evaluated under the assumptions that the attacker knows all details of the algorithm and the system it is used within. The only thing the attacker doesn't know is the key. Of course, keeping the algorithm secret gives an extra layer of protection. However, the history of GSM shows that keeping an algorithm implemented and used in so many places is very difficult to achieve and claims about the algorithm structure tend to be published.

Of course the trust in an algorithm is dependent of the trust you have in its evaluators. But an open algorithm that has undergone public review should incur more trust of the end users in the design.

The competitive situation should also be considered. TIA TR-45 is working on security enhancements in present systems and security architecture for 3G. The strategy adopted is to request proposals with open algorithms.

Possible choices.

1. Open algorithms

2. Secret algorithms

Assumptions:

1. Competitive situation is better with open algorithms.

2. Trust is higher in open algorithms.

3. It is very difficult to keep secret algorithms secret.

4. If a design flaw in a secret algorithm is detected and published, the trust is seriously hurt.

5. Open algorithms are always open for analysis, which may result in publication of attacks that are only of theoretical interest.

4.4 Design Strategy

The possible design strategies are discussed in the following three clauses. They are

Possibilities:

1. Select an of the shelf algorithm.

2. Invite submissions

3. Commission a special group to design an algorithm

4.4.1 Select an off the shelf algorithm

Under this heading we only consider the selection based on the suitability of the algorithm for its use and implementation in the system. The evaluation of its security is treated elsewhere. The experts performing the selection doesn't necessarily need to be experts in cryptology but in system aspects. They are probably available within 3GPP.

Assumptions:

1. The expertise needed for evaluating suitability is available.

2. The selection process will not be too time-consuming (appr. 2 month).

3. There exists candidates (e.g. ETSI secret algorithms, open FIPS standards and AES candidates)

4. There is no difference between selecting secret or open algorithms.

4.4.2 Invite submissions

Interested parties, within and outside 3GPP, are invited to submit proposals. Of course, the success of the approach relies on the willingness from the interested parties to submit proposals. (TIA TR-45 did this. How many were proposals were submitted?) This approach is mainly used for open algorithms but it would be possible to invite submissions for secret algorithms.

The time from issuing the RFP till deadline for submissions in a world-wide environment should be at least 6 month. The number of submitted proposals will be dependent on the response time. Thus there is a certain minimum response time to get any proposals at all.

If there are several proposals (but also in case of a single proposal) an evaluation/selection regarding suitability has to be performed.

Assumptions:

1. Interest to submit proposals is limited but present.

2. The time from issuing the RFP till deadline for submissions should be at least 6 month

3. The expertise needed for evaluating suitability is available.

4. The selection process will not be too time-consuming, 2-3 month. However if the algorithm should also be open to public scrutiny the selection process will be much longer, more like a year or even longer

4.4.3 Commission a special group to design an algorithm

A group of crypto experts are commissioned to develop an algorithm, open or secret. Here the availability of experts, trusted by all, is one issue. A certain time (4 month) is also needed for the design.

As the algorithm is a special purpose design according to a specification its suitability should be guaranteed.

The more algorithms to design the more experts are needed.

Assumptions:

1. Crypto experts for the design are available.

2. Trust will be high if the algorithm is open and the design principles published.

3. A secret algorithm will have a lower trust level.

4. The suitability of the algorithm is high

5. Time for design is at least 4 month

4.5 Evaluation Strategy

As stated above, the available methods for evaluation are either to rely on voluntary efforts or to commission a group of experts. The evaluators would of course review any existing evaluation reports and do their own analysis.

To rely on voluntary efforts and existing available security statements is probably not sufficient. A group of experts has probably to be assigned (commissioned) to perform the evaluation. Expertise might be scarce but it will probably be possible to have such a group. The minimum time needed for the security evaluation would be approximatel4 month.

If the algorithm is open, the performed analysis methods and results may be published together with the evaluation report. This should give greater trust in the algorithm. If the evaluation is of a secret algorithm or if just the conclusions are published the trust in the algorithm will to a large extent depend on the trust in the experts.

The more algorithms to design the more experts are needed.

Assumptions:

1. The needed expertise is scarce but available on a commissioned basis.

2. The time for evaluation is at least 6 month for a new design and 2 for an off the shelf algorithm that has been seriously analysed in the open literature. However if the algorithm should also be open to public scrutiny the selection process will be much longer, more like a year or even longer.

3. The trust will be higher with a public evaluation report.

4.6 Evaluation Strategy

The algorithm specifications could be distributed in the following ways.

1. No distribution; refer only to existing specification including test data

2. Refer to existing specification; distribute test data

3. Restricted distribution of specification and test data through custodian

Methods 1 & 2 are only possible for open algorithms and 3 is the only choice for secret algorithms. 1 is very simple and 3 requires that someone do all admin.

5 Possible algorithm design process scenarios

This clause will provide a number of example scenarios for the algorithm specification process. Many more scenarios are possible, but the ones presented below provide a good indication of the possibilities.

5.1 Use of a public off the shelf algorithm

This section describes a scenario in which a public algorithm, which to a large extend fulfils the specified requirements, is selected.

Possible procedure:

1. A group identifies that a certain public algorithms fulfils the requirements

2. This group selects an algorithm (possibly after consulting other groups) or asks another group to make this selection on their behalf

3. A formal 3GPP specification is drafted

Time/effort needed

Step 1: 1-2 months; committee effort

Step 2: 1-2 months; committee effort or 2-4 months task force

Step 3: 2 months; committee effort or 2-3 month's task force

Total time: at most 6 months and at most 6 months task force

5.2 Select a confidential off the shelf algorithm

The idea is to use a public algorithm and modified in a specific confidential way without the need to have a full analysis of the algorithm. (So a public algorithm is used to create a confidential algorithm which has undergone public scrutiny).

Possible procedure:

1. A group identifies that a certain public algorithm that could be used as basis for the confidential algorithm

2. This group selects an algorithm (possibly after consulting other groups) or asks another group to make this selection on their behalf

3. A group is asked to make the modifications to the algorithm and carry out a brief analysis to check that these do not affect the security.

4. A formal 3GPP specification is drafted

Time/effort needed

Step 1: 1-2 months; committee effort

Step 2: 1-2 months; committee effort or 2-4 months task force

Step 3: 2-3 months; 2-3 month's committee effort

Step 3: 2 months; committee effort or 2-3 month's task force

Total time: at most 8 months and at most 9 months task force.

5.3 Invite submissions for algorithms

Possible procedure:

1. A group identifies that a certain public algorithms that could be used as basis for the confidential algorithm

2. This group selects an algorithm (possibly after consulting other groups) or asks another group to make this selection on their behalf

3. A group is asked to make the modifications to the algorithm and carry out a brief analysis to check that these do not affect the security.

4. A formal 3GPP specification is drafted

Time/effort needed

Step 1: 1-2 months; committee effort

Step 2: 1-2 months; committee effort or 2-4 months task force

Step 3: 2-3 months; 2-3 month's committee effort

Step 3: 2 months; committee effort or 2-3 month's task force

Total time: at most 8 months and at most 9 months task force.

Here the call could be made for proposals from 3GPP members, to speed things up.

5.4 Commission a special group to design an algorithm

Possible procedure:

1. A special group is commissioned to develop the algorithm. They may base the design on an existing algorithm or start from scratch.
2. A special group of experts is also commissioned to for the evaluation of the algorithm.
3. A formal 3GPP specification is drafted.

Time/effort needed

Step 1: 3-4 month, task force.

Step 2: 2-3 month, task force.

Step 3: 2 month, task force, most of the work can be done in parallel with step 2

The algorithm may be kept secret during the design and evaluation phases and then after be made public or remain to be secret.

6 Relevant aspects in an algorithm acquisition process

Below the relevant aspects in the design process are summarised in the form of two tables. The first table contains the design and the second one the evaluation process.

6.1 Design methodology

The options for the algorithm design are the following options.

1. Select a public of the shelf algorithm
2. Select a confidential of the shelf algorithm
3. Invite submissions for an algorithm
4. Commission a special to design an algorithm

Opt ion	Public trust in algorithm	Time needed	Availability (of experts / algorithms)	IPR problems or protected	Tailored for use / Suitability	Guarantee of strength	
1	+	0	-/0	-/0	0	+	
2	-/0 Depends on evaluation	+	-/0	0	0	0 Depends on evaluation	
3	+	-	+	0	+	+	
4	-/0 Depends on evaluation	+	+	+	+	0 Depends on evaluation	

6.2 Evaluation methodology

The options for the evaluation of a proposed selected algorithm are the following.

1. Expert evaluation
2. Publication with request to respond
3. Review of existing analysis

Opt ion	Public trust in algorithm	Time needed	Availability (of experts or analysis)	Guarantee of strength			
1	0/+ depending on experts	0	0/+	0/+			
2	+	-	+	+			
3	0/+	+	-/0	0/+			

7 Conclusions and recommendation

In view of what has been described above and the requirements on a speedy process, both algorithms should be ready by December 1999, the scenario 5.4 with a commissioned group designing the algorithms and one or more commissioned groups evaluating , seems to be the only viable solution. The algorithms should in the end be made public (after the expert evaluation is finished) to achieve maximum public trust in the systems.

ETSI SAGE should be the design authority for the algorithms. It is expected that the project team assembled by SAGE will draw upon appropriate expertise within the 3GPP partner organisations in addition to its normal resource pool of experts.

One question, which remains to be answered is about whom will take on the responsibility for the algorithms.

Appendix 1– Overview of ETSI Standard Algorithms

This annex will list a number of systems developed by ETSI and describe the algorithms that are used in those standards

GSM – the Global System for Mobile communications

GSM was the first public standard digital telecommunication system with a substantial amount of cryptography integrated. The system originally used a standard encryption algorithm called A5 (later this became A5-1) which is used for the encryption of user and signalling data over the radio path. The A5-1 encryption algorithm was not developed by SAGE (SAGE did not exist at the time it was developed) but by a special group: the GSM Algorithm Expert Group (AEG).

Originally A5-1 was used in every GSM system, but when GSM started to expand outside Europe, the use of A5-1 in some cases turned out to be impossible because of controls on the export of the algorithm to certain countries. To overcome these export control problems, an alternative A5-2 encryption algorithm was developed, in this case by ETSI SAGE. However, the algorithm mostly used in GSM is A5-1.

The GSM system also uses an algorithm for authentication and encryption key generation. This algorithm is called A3/A8. It is not a standard algorithm and operators are free to choose or develop their own. For those operators who do not want to do this an example A3/A8 algorithm with the name COMP128, developed by the GSM AEG, used to be available from the GSM Association. In 1998 this algorithm was compromised and from the start of 1999 COMP128 has been replaced by another GSM Association example algorithm.

For the new GSM data service, the General Packet Radio Service (GPRS), a special encryption algorithm had to be developed (GPRS data is encrypted on a different level as regular GSM user and signalling data). This algorithm is called the GPRS Encryption Algorithm (GEA) and was developed by SAGE.

Furthermore it is planned that SAGE in 1999 will design a special set authentication, key generation and integrity algorithms for another new GSM service, GSM Cordless Telephone System (CTS).

DECT – Digital Enhanced Cordless Telecommunications

DECT has security features that are similar to those in GSM. Just like GSM it uses an encryption algorithm, the DECT Standard Cipher (DSC), and an authentication and encryption key generation algorithm, the DECT Standard Authentication Algorithm (DSAA).

Both algorithms were not developed by ETSI SAGE (which did not exist at the time of the development) but by special ETSI project teams.

The DSC and DSAA both are about 8 years old now and recently it was decided to make the algorithm available to ETSI SAGE, which should review if the algorithms still are suitable for their use.

ISDN based audio-visual system

CCITT has drafted recommendation H221, H261 and H233 in the area of the use of audio-visual systems and the security for these. The CCITT recommendations were adopted by ETSI as standards.

Recommendation H233 (“Confidentiality for audio-visual services”) specifies the use of encryption algorithms. In fact it allows different algorithms to be used. ETSI SAGE specified an encryption algorithm especially for this purpose. It is called BARAS (Baseline Algorithm Recommended for Audio-visual Services).

Multi-application telecommunications cards

Several years ago a sub committee of the ETSI TC Terminal Equipment (TE) drafted a series of standards for a Multi-application Telecommunications IC (Smart) Card. The specifications included a number of security functions.

To support these security functions, ETSI SAGE designed and specified a cryptographic algorithm called TESA-7. The specification included four modes of use for the algorithm. These are an authentication mode, an integrity mode, a key diversification mode (i.e. calculating an individual key from an identity and a master key) and a secure (encrypted) key loading mode.

The standards for the Multi-application Telecommunication IC Card have not been very successful and the TESA-7 algorithm is therefore hardly used.

Recently there has been a proposal to broaden the use of TESA-7 to the GSM SIM (Subscriber Identity Module - the smart card of GSM). This broadening will probably be formalised in the first half of 1999.

UPT – User Personal Telecommunications

UPT is a telecommunication service standardised by ETSI that enables user to register on a telephone and then be reached there under their own telephone number. This service requires authentication before it can be invoked.

ETSI SAGE designed the standard authentication algorithm, called USA-4, for this services. However, until now, the UPT standard and hence the USA-4 is not used very often.

Hiperlan – High Performance Radio Lan

Hiperlan is a standard for a radio lan over which data is transmitted at high speeds over the air interface. For this standard SAGE developed an encryption algorithm HSEA (Hiperlan Standard Encryption Algorithm). The export restrictions on the algorithm are minimal (this was an important requirement when the algorithm was designed) and it provides a basic level of security.

ETSI Project BRAN is currently standardising a successor (called BRAN) for Hiperlan. This will support higher speeds and very probably also employ a standard encryption algorithm.

BEANO - Binary Encryption Algorithm for Network Operators

A few years ago ETSI TC Security identified the need for an algorithm that could be used to protect the confidentiality of network management data. ETSI SAGE designed a special encryption algorithm called BEANO (Binary Encryption Algorithm for Network Operators). To overcome the conflicting requirements for a broad exportability and a very high level of security the licence and confidentiality agreement explicitly limits the use of the algorithm to the protection of network management data. The use of the algorithm for other purposes such as the protection of user data is explicitly excluded.

The algorithm is not used at the moment. The reason for this is that the security work of ETSI TMN (Telecommunications Management Network), the group responsible for drafting the standards in which the algorithm is supposed to be used, is delayed.

TETRA – Terrestrial Trunked Radio

TETRA is the standard for a new digital private mobile radio communications system. It can be used in public networks but also it is selected by the major Public Safety organisations in Europe as their future mobile communications system. Clearly for the latter user groups security has a high priority and therefore TETRA includes a large number of security features. These are supported by a number of standard cryptographic algorithms. There a two standard TETRA Encryption Algorithms TEA1 and TEA2. TEA1 is for general use in TETRA systems and it provides a basic level of security. The use of TEA2 is restricted to European Public Safety organisations (mainly from the "Schengen" countries). Because TEA1 and TEA2 do not cover the whole portfolio of encryption algorithms which are needed and SAGE will design two further standard encryption algorithms.

Furthermore SAGE has specified one set of TETRA Authentication and key management Algorithms (TAA1). The TAA1 is designed for use in all TETRA systems.