3GPP TSG SA WG3 Security — S3#16 **S3-000705**

28-30 November, 2000

Sophia Antipolis, France

TIPHON 21
Kyoto, Japan
December 4-8, 2000

Temporary Document 036
page 1 of 16

Source: STF114, Scott

Title: **Authentication framework and algorithm boundary conditions**

Notice: The author of this document declares that ETSI **may** make the document publicly available.

Document for:

Decision:	X
Discussion:	X
Meeting Report:	
Liaison:	
Information:	

Contact details:

First Name, Last Name Scott W Cadzow
e-mail: Scott.Cadzow@etsi.fr

1. Decision/Action Requested

To approve the attached text as content of WI-08004.

To add the functional elements and information flows into the TIPHON architecture. The document proposes a "kerberos" like framework for authentication with a secret key relationship using a single registration identity to key mapping. The resulting token shall however take the form of an authentication derived encryption key that is shared with the application server and used to encrypt every message. The encryption mechanism favoured is the Encrypted Security Payload in tunnel mode of IP-Sec. To support this the document proposes also a "registration identity" which is analogous to the IMSI of GSM or ITSI of TETRA.

This paper identifies the appropriate documents that individual requirements should appear in (this is assuming that not all counter-measures to the risks/threats identified in DTR/TIPHON-08002 are explicit security measures).

In addition the document considers the public key framework that provides security for OSP.

2. Definitions

Authenticatee	The entity that is making a claim.
Authenticator	The entity that makes the decision that the authenticatee is as claimed
Claimant	See also authenticatee
Verifier	See also authenticator
Signer	See also authenticatee

3. References

4. Contents

5. Introduction

Security is not about the magic of cryptography which can use maths to secure messages and confirm knowledge of secrets. Whilst such tools play a significant part in enforcing security the more important aspect in an environment such as TIPHON is to ensure that functional elements within the architecture do the job required of them in a closed loop. In other words the base architecture and protocols need to asses their own risk and counter risks inherent in misaligned messages or misdirected messages. Having said all of this security in TIPHON consists of three algorithmic or cryptographic methods:

Authentication – to counter masquerade and as a tool in authorisation

Encryption – to offer privacy

Integrity – to determine if a message has been altered.

Much of the content of TIPHON's signalling has to be transmitted in clear although this can be successively added or stripped away. Each of these methods can be applied at different layers in each of the planes. There is also the need to isolate domains within each of the planes and to consider how security management is enabled across domain borders.

The dominant threats in TIPHON are related to confirmation of the identity, transfer of data and its protection from eavesdropping and analysis, and privacy of the communications made by a user. In addition it is important that signalling data can be assumed to have been unaltered whilst on the path from source to destination. If measures are provided to ensure these threats are removed then the overall security of TIPHON may be considered good.

6. Summary of threat analysis (risk assessment)

The following attacks are categorised as moving TIPHON into the region of critical risk:

Table 7: Risk factors for TIPHON network architecture

	Attack scenario	Threat Reference	Possible occurrence of threats	Motivation	L	I	R
Denial of Service							
1	Flooding the target for Denial of Service	8.1.1	T, GK, MGC T1, T2	sabotage, attacker satisfaction	3	3	9
2	Modifying stored information	8.1.1	GK, UP, BRF S2, SC2, R1, R2, C1, C2	sabotage, disabling and harming of individual subscribers, attacker satisfaction	2	3	6
3	Physical removing of resources	8.1.1	all reference points	sabotage, disabling and harming of individual subscribers, attacker satisfaction	2	3	6
Eavesdropping							
5	attaching a protocol analyser to any accessible link	8.1.2	all reference points	espionage, getting information (e.g. prerequisite for masquerade and sabotage) , attacker satisfaction	2-3	2-3	4-9
Masquerade							
8	Hijacking a link after authentication has been performed.	8.1.3	GK, SGW	fraud, harming subscribers, sabotage, getting information, attacker satisfaction	2	3	6
9	using authentication information which has been obtained by eavesdropping.	8.1.3		fraud, harming subscribers, sabotage, getting information, attacker satisfaction	3	3	9
Unauthorised access							
10	exploiting system weaknesses	8.1.4		Fraud, harming providers, sabotage, getting information, attacker satisfaction	2-3	2-3	4-9
11	masquerading as an entity with higher access permission	8.1.4		fraud, harming providers, sabotage, getting information, attacker satisfaction	1-2	2-3	2-6
Loss of information							
12	(deliberate) deletion of data	8.1.5		sabotage, harming providers and individual subscribers, fraud	1-2	3	3-6

	Attack scenario	Threat Reference	Possible occurrence of threats	Motivation	L	I	R
13	modification of access rights of other parties	8.1.5		harming providers and individual subscribers	2-3	3	6-9

			Corruption of information				
15	modifying stored information	8.1.6		sabotage, harming providers and individual subscribers	2	3	6
			Repudiation				
19	denial of having accessed data in a database	8.1.7		fraud, sabotage	1-2	3	3-6
20	denial of having modified data in a database	8.1.7		fraud, sabotage	1-2	3	3-6

7. Risk reduction methods

7.1 Denial of Service attacks

To be provided in the transport plane by enforcement of the following rules:

- Disable of IP directed broadcast
- Disable response to ICMP messages sent to broadcast addresses

This requirement enforces default router behaviour to that described in RFC2644. In making this modification the DOS attack is not propagated to the service plane. This requirement has to be mandatory for all TIPHON transport plane elements.

ADD TO TRANSPORT LAYER REQUIREMENTS (DTR/TIPHON-01006)

7.2 Modifying stored information

Information in TIPHON is required only for use by the communications protocols contained under the umbrella of TIPHON. The following rule shall provide an initial protection of data:

- Data shall only be accessed by validated protocols

The protocols themselves shall contain sufficient data to allow source verification (by address or identity) and thus the protocol shall enforce access control. This shall include the provisioning phase enabled by management protocols.

7.3 Eavesdropping

In a TIPHON environment there will be open interfaces (i.e. not physically protected) and in such instances the only effective method of achieving confidentiality is to encrypt the traffic flows. However encryption of packet media in streaming protocols requires that the headers remain in clear (unless a VPN form of tunnel is established between the end points).

7.4 Masquerade

Countering masquerade really requires authentication. This can take many forms. Authentication is optional but where implemented a single standardised method and algorithm set should be used (to achieve maximum interoperability).

7.4.1 Authentication by private key

The two agencies being authenticated share knowledge of a single secret. Proof of this knowledge is exchanged in a multi-pass protocol exchange using parameters that when combined algorithmically with the key provide a result that can be exchanged. An attack of the key affects only one user (at attack on the key centre though affects all keys stored in that centre).

7.4.2 Authentication by public key

This consists of using a two part key. One part is public and the other is private. Any action taken by one can only be undone by the other. Very popular in e-commerce where the public part is given out in a site certificate and the vendor information is encrypted using this key which can only be decrypted by the holder of the private part of the key. The risk in this form of system is that breaking the key pair (i.e. finding the private key attacks the confidentiality of all users of the public key and thus can be used to attack public or utility sites such as OSP brokers, although most key pairs are difficult to break).

8. Structure of TIPHON security document

The following structure is proposed for TIPHON security. It is based upon the need to support the CIA of security:

Confidentiality;

Integrity; and,

Authenticity.

The document then proposes to further split each of these functions into a number of testable and specifiable areas:

Access to TIPHON

Intra domain security

Inter domain security

It is proposed to further subdivide each of these areas into Circuit Switched and IP technology areas.

8.1 Frameworks

TIPHON is not a network but an environment and as such it has to provide a framework for interoperability. The security draft standard therefore proposes a framework for authentication, key management and encryption.

9. Architecture considerations

There are basically 2 architectural modes of operation:

Connect to Authentication server and be authorised to use an application server

Connect to an application server and be authenticated by that as a proxy

The second of these two options is more suited to TIPHON. This allows an application server to exist at the virtual network edge

Registration shall be the trigger for authentication and the registration server (at the home or visited domain) shall act as a proxy to the authentication service. In order to maximise the security of this the authentication algorithm should be in two parts in order for the key data to be maintained only in the authentication server.

We need to start with the working assumption that the authentication server is always in a different domain from the application server. This means we can make it co-located if we wish but to start with the assumption it is co-located will make any design that later re-locates the servers difficult.

There will be 2 protocols in the architecture:

Terminal to authentication proxy

Authentication proxy to authentication server

The exchange of authorisation data within a "token" shall be carried out by the registration server

10. Overview

10.1 Authentication framework

Authentication in TIPHON is optional but if implemented shall use the framework and algorithms specified in this TS.

Entities that should be authenticated are as follows:

- Terminals with dynamically provisioned parameters
- Functional elements within the network with dynamically provisioned parameters
- Terminals with variable point of network attachment
- Terminals with variable point of service attachment
- Functional elements within the network with variable point of network attachment
- Functional elements within the network with variable point of service attachment

The TIPHON authentication framework is loosely based upon the Kerberos framework described in RFC1510 []. The TIPHON framework provides support to the native authentication mechanisms in GSM [], DECT [] and TETRA [] and establishes a framework for use by SIP [] and H.323 []. The TIPHON authentication framework shall support strong secret key authentication.

The authentication framework supports a TIPHON authentication service between peer entities in the TIPHON environment.

The authentication framework may be used to provide keys for use by the encryption service described in the encryption framework.

NOTE: This TS does not define the algorithms to be used for authentication but does specify the boundary constraints for the algorithms.

Figure 1 shows in MSC format the kerberos protocol.

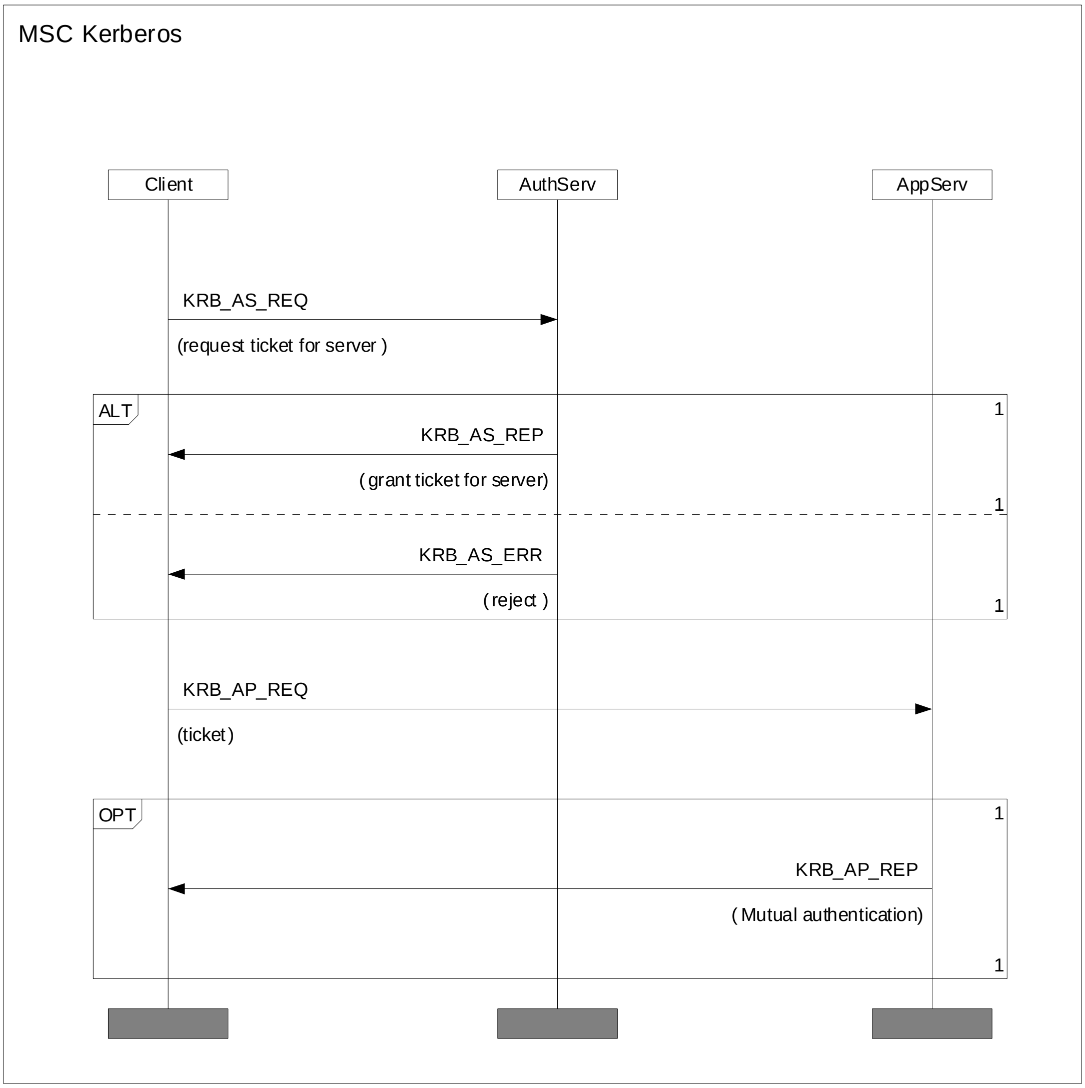

Figure 1: Simplified Kerberos protocol exchange

Every message sent from the client to the application server refers to the ticket and the ticket tells the application server that this client is allowed to invoke the referred application. No ticket, no invocation.

Kerberos requires that the authentication server maintain the secret keys of each client and each application server. The derivation of a TIPHON authentication framework from Kerberos is shown in figure 2 (this will need further study).

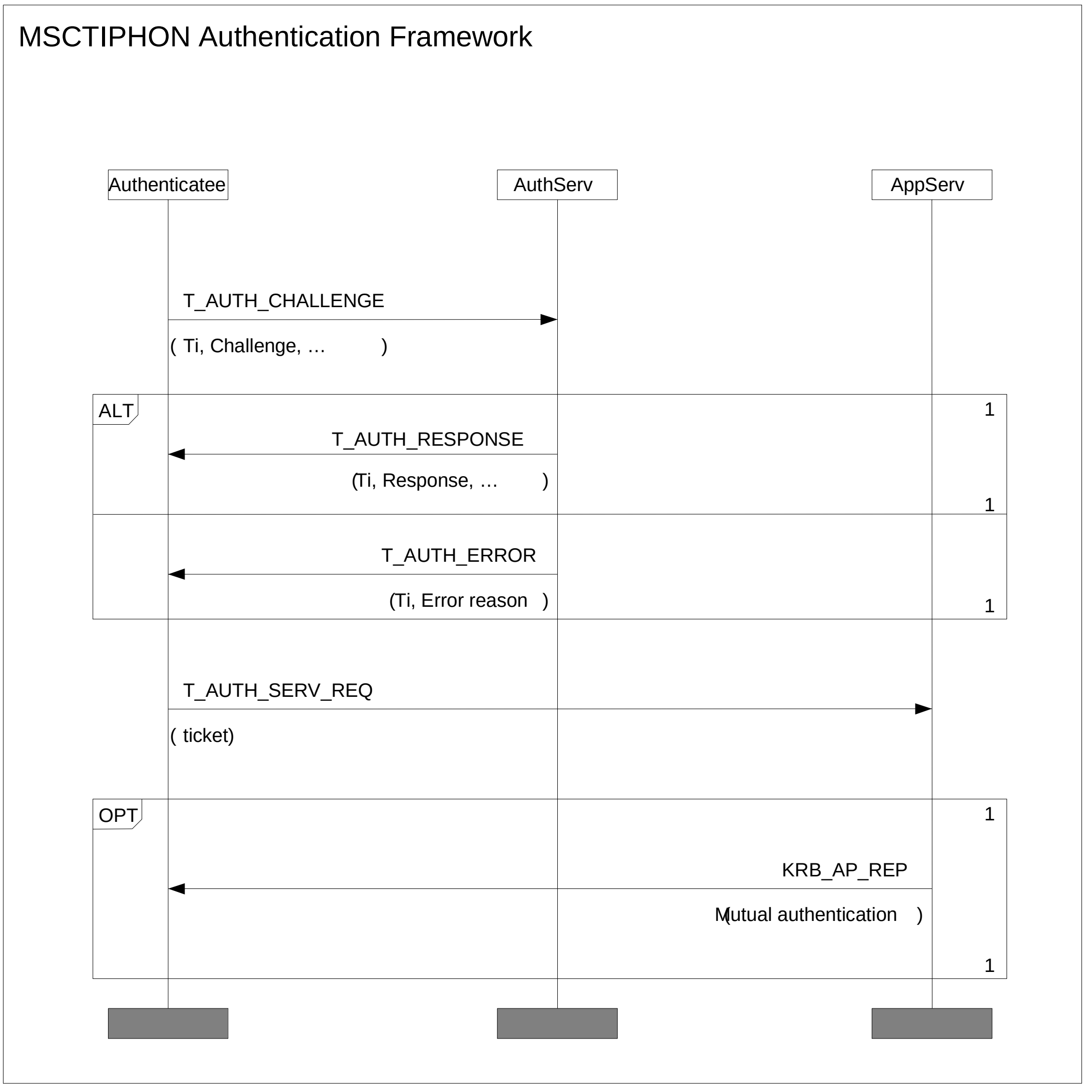

Figure 2: TIPHON authentication framework (ffs)

A more complete view of the overall environment in which authentication takes place is given in figure x:

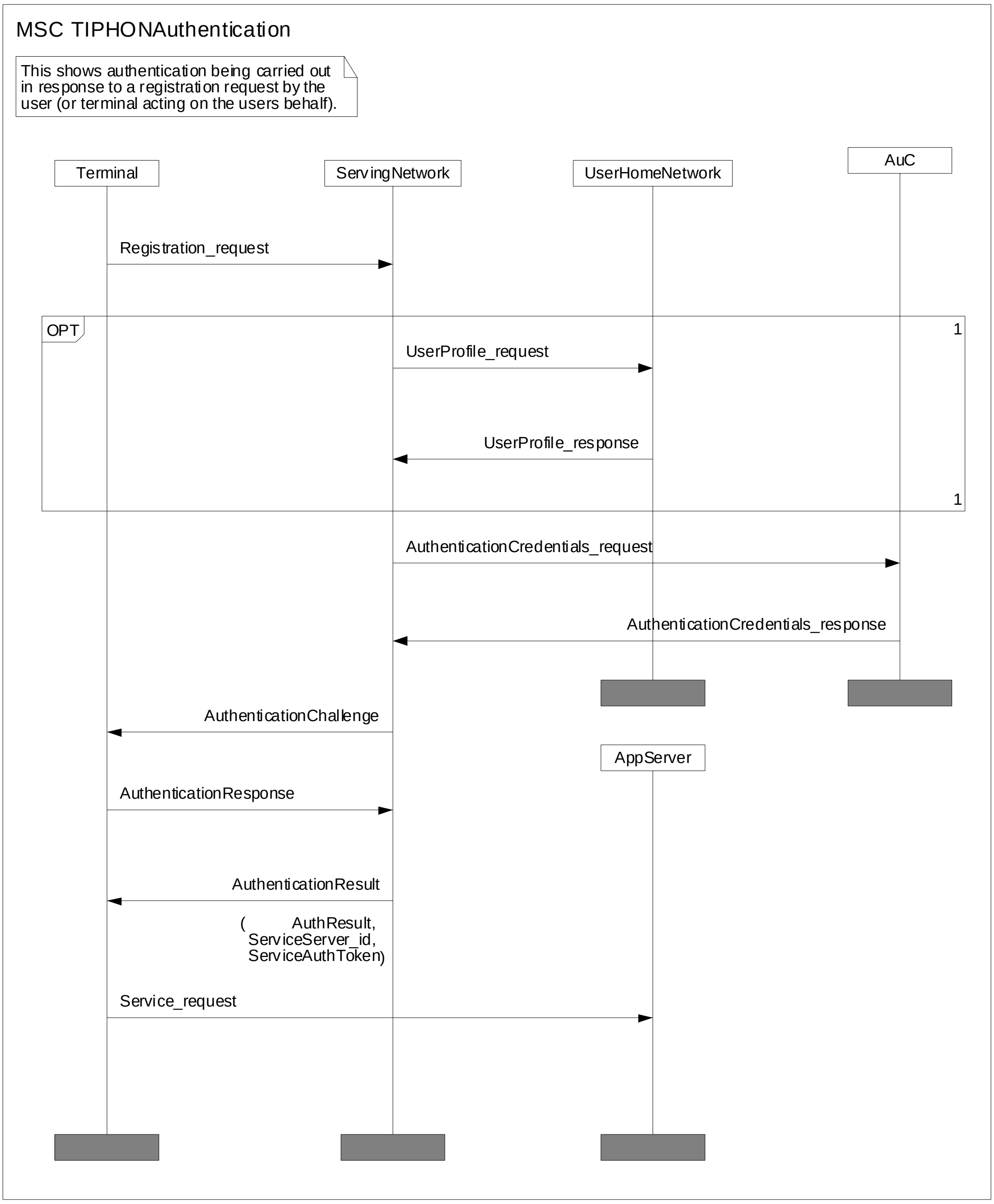
MSC TIPHONAuthentication
This shows authentication being carried out in response to a registration request by the user (or terminal acting on the users behalf).
Terminal
ServingNetwork
UserHomeNetwork
AuC
Registration_request
OPT
1
UserProfile_request
UserProfile_response
1
AuthenticationCredentials_request
AuthenticationCredentials_response
AuthenticationChallenge
AppServer
AuthenticationResponse
AuthenticationResult
(AuthResult, ServiceServer_id, ServiceAuthToken)
Service_request

Figure 3: TIPHON authentication in context of other TIPHON elements (ffs)

In the above picture the registration request is followed by recovery of the user profile. This profile should show the applications that the user is allowed to access and the location of the authentication server for the user. Once the authentication server is known the serving network requests the authentication credentials for the user

The authentication itself is a straightforward challenge-response type with the result giving the token credentials for each service to be used by the authenticated user. The services to be offered have to exist in the profile and on successful authentication the result to the user indicates how to reach these services securely (i.e. such that the application server knows that the request comes from an authenticated source).

10.2 Authentication service

The authentication service requires 3 states to be synchronised between the authenticatee and authenticator as follows:

- Not Authenticated: Only registration and authentication services allowed
- Authentication Pending: Only authentication flows allowed
- Authenticated: All services authorised in the current profile opened

If the authentication protocol fails to complete within some time TA the authenticating parties shall each revert to the security state that was in place prior to the start of the authentication protocol.

The authentication protocol shall have the following properties:

- bi-directional challenge-response type
- able to be initiated either explicitly or as part of the registration procedure.
- able to be initiated by the terminal or the network
- The recipient of the first authentication demand may instigate mutual authentication by use of a mutual authentication indicator, and by sending its challenge together with the response to the first challenge.
- Where authentication is initiated as part of the registration the authentication timer TA shall always be less than or equal in value to any registration timer

10.3 Authentication algorithms and key management

The boundary conditions only shall be set by TIPHON based at least on the following criteria:

- Current and forecast cryptanalysis capability;
- Exportable key-length constraints;
- Lifetime for which data has to be kept secure.

Each unique TIPHON identity (Ti) shall have a one-to-one mapping to a secret key (Kt).

Characteristics of TIPHON identity:

- Unique (globally)
- Identifies home service

-Identifies geographic location

-Identifies service provider

Approximate requirements on key length can be obtained by consideration of the budget of the attacker and from extrapolation of computing power from Moore's Law.

Table x: Time to break secret key encrypted message using brute force (January 1996 figures)

Attacker profile and budget	**Key length**		
	56	**64**	**90**
Individual, $10k	1 year	>100 years	-
Large organisation, $10M	few days	1Year	-
Government agency, $300M	Seconds	Minutes	>100 years

Extrapolation from the above table suggests that for data to remain relatively invulnerable to brute force attack until the year 2050 (i.e. for 50 years) in which the computing power will increase (for fixed cost) by a factor of (approximately) 1 billion (or 2^{33} times) suggests that a key length in excess of 96 bits is required.

NOTE 1: The possible evolution of quantum computing will invalidate all of these figures.

NOTE 2: Successful attacks on algorithms and key management will invalidate all of these figures.

The same boundary condition algorithm for authentication in a challenge response protocol is slightly different. In practice the algorithm is known to the attacker as is the challenge and the response, the latter can be captured in transit.

10.4 Algorithm set for TIPHON

The authentication on the TIPHON server side is split into 2 (part at the authentication server, part at the registration server). This suggests a 2 part algorithm in which the secret needs to be maintained only at the server.

- Algorithm 1 shall calculate a session key and some random data.
- Algorithm 2 shall use the session key to determine an expected response to the authentication challenge using the challenge as one of the inputs.

I propose that one of the outputs of algorithm 2 will be the key to be used in future exchanges with application servers.

NOTE: This is very much the scheme used in GSM. DECT and TETRA in which the authentication exchange derives an encryption key. Using this encryption key then provides authentication of each packet encrypted with it.

10.5 Mapping authentication framework to architecture

The TIPHON architecture shall contain an authentication server functional entity with the following capabilities:

Shall maintain a database of principals and their keys.

The application server shall map to the following technology specific entities:

- H.323 gatekeeper

- SIP server
- GSM HLR/VLR
- 3G HSS/VSS
- …

10.6 Encryption framework

The encryption mechanism in TIPHON shall use authen

10.7 Integrity checking framework

11. Terminal to Network security

11.1 Authentication & Key Management

11.1.1 SCN Terminals

11.1.1.1 GSM Terminals

Shall use the IMSI authentication methods described in [3,4,5].

11.1.1.2 GPRS Terminals

Shall use the IMSI authentication methods described in [3,4,5].

11.1.1.3 TETRA Terminals

Shall use the authentication methods described in EN 300 392-7 [7] appropriate to the class of the TETRA network. It is recommended that operation is with authentication applied (i.e. at class 3, or at class 2 with authentication, or at class 1 with authentication).

11.1.1.4 DECT Terminals

Shall use the authentication methods described in [6].

11.1.1.5 ISDN Terminals

No authentication mechanism is defined for ISDN terminals.

11.1.1.6 PSTN (analog) terminals

No authentication mechanism is defined for ISDN terminals.

11.1.1.7 3G mobile terminals

ffs.

11.1.2 IP Application Terminals

11.1.2.1 SIP Terminals

11.1.2.2 H.323 Terminals

11.2 Encryption

11.2.1 SCN Terminals

11.2.1.1 GSM Terminals

Shall use the encryption methods described in [3,4,5].

11.2.1.2 GPRS Terminals

Shall use the encryption methods described in [3,4,5].

11.2.1.3 TETRA Terminals

Shall use the encryption methods described in EN 300 392-7 [7] appropriate to the class of the TETRA network. It is recommended that TETRA class 3 is used as this provides implicit authentication for every received packet.

11.2.1.4 DECT Terminals

Shall use the encryption methods described in [6].

11.2.1.5 ISDN Terminals

No encryption mechanism is defined for ISDN terminals.

11.2.1.6 PSTN (analog) terminals

No encryption mechanism is defined for ISDN terminals.

11.2.2 IP Application Terminals

11.2.2.1 5.1.2.1 SIP Terminals

11.2.2.2 5.1.2.2 H.323 Terminals

12. Intra Network security

Ffs

13. Network element to Border Element security

Ffs

14. Inter network security through Border Elements

ffs

15. Security of TIPHON abstract services

A terminal is used (by the end-user) to access TIPHON through an access network. The security of the access network is not addressed directly in TIPHON. However, access networks provide a link into the TIPHON environment and therefore any security service offered within the TIPHON environment has to be reflected in the access network.

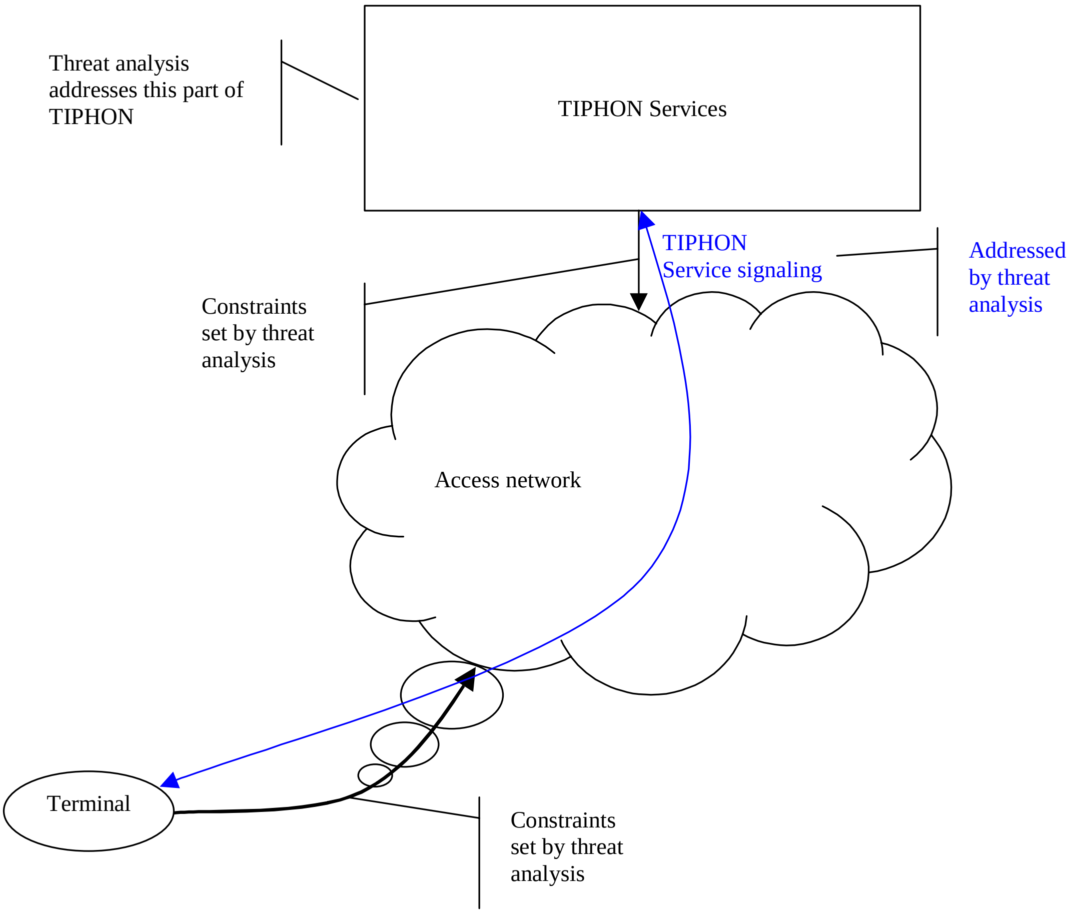
Threat analysis addresses this part of TIPHON
TIPHON Services
TIPHON Service signaling
Addressed by threat analysis
Constraints set by threat analysis
Access network
Terminal
Constraints set by threat analysis

Figure 4: Security model

It is noted by the diagram that the route through the access network to the TIPHON services does not need to be defined in TIPHON. This means that routing and switching networks can be treated in like manner.

16. Discussion

17. Conclusion