SLOVENSKI STANDARD
SIST-V ETSI/EG 201 510 V1.1.2:2003

01-november-2003

Inteligentno omrežje (IN) - Varnostni vidiki funkcije krmiljenja storitev (SCF) - Funkcija komutacije storitve (SSF) medsebojnega povezovanja omrežij - Operacije na podlagi prvega nabora zmožnosti (CS1)

Intelligent Network (IN) - Security aspects of Switching Control Function (SCF) - Service Switching Function (SSF) interconnection between networks - Part 1: Capability Set 1 (CS1) based operations

Ta slovenski standard je istoveten z: EG 201 510 Version 1.1.2

ICS:

33.040.35	Telefonska omrežja	Telephone networks

SIST-V ETSI/EG 201 510 V1.1.2:2003 en

ETSI EG 201 510 V1.1.2 (2000-05)

ETSI Guide

Intelligent Network (IN);
Security aspects of Switching Control Function (SCF) - Service Switching Function (SSF) interconnection between networks;
Part 1: Capability Set 1 (CS1) based operations

Reference

DEG/SPAN-061212-1

Keywords

CS1, IN, interworking, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

The present document is part 1 of a multi-part EG covering the Intelligent Network (IN); Security aspects of Switching Control Function (SCF) - Service Switching Function (SSF) interconnection between networks, as identified below:

Part 1: "Capability Set 1 (CS1) based operations";

Part 2: "Capability Set 2 (CS2) based operations".

Introduction

Under IN CS1 and CS2, the IN SCP to SSP relationship, or Service Control to Switch, is confined to a single network operator's domain and may actually be physically co-located as an SSCP. To optimize performance, the switch requires little security, particularly if implemented within a 'single unit' or SSCP. By not using the local processor for security, switch performance may be optimized toward call processing with security and network protection measures provided at the Service Control Point.

In the case of inter-connected networks, direct implementation of the Inter-network Control to Switch relationship would require appropriate security and authentication measures to be provided and managed at each SSF.

Within a single network, potential conflict between multiple SCFs is avoided by their management within a common domain. When two networks are interconnected two (or more) SCFs in different domains can potentially control the same resource (SSF). Then some secure resource allocation and management procedure must be deployed. Suitable mechanisms have not yet been standardized. Network operators may prefer the option of utilizing the established inter-network SCF to SCF security procedures and route inter-network service switching signalling messages via each Network's Service Control Point. In this case appropriate security and authentication measures would be provided and managed at each SCF.

1 Scope

The present document describes security aspects in conjunction with the interconnection of two IN structured networks. The present document concentrates on the SCF - SSF interconnection.

The purpose of the present document is to describe the security aspects of interconnection of SCF to SSF. The operations considered in this interconnection are a subset of CS1. For the time being CAMEL is the only application of SCF - SSF interconnection, therefore the present document considers only CAMEL phase 1 operations. A later edition may also consider other CS1 operations.

Future parts of the present document will investigate the security aspects of operation sets that are a subset of CS2 and CS3.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ITU-T Recommendation Q.1228 (1997): "Interface Recommendation for intelligent network Capability Set 2".

[2] ETSI ETR 232: "Security Techniques Advisory Group (STAG); Glossary of security terminology".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

masquerade ("spoofing"): pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery

unauthorized access: entity attempts to access data in violation to the security policy in force

eavesdropping: breach of confidentiality by monitoring communication

loss or corruption of information: integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay

replay of information: repetition of previously valid commands and responses with the intention of corrupting service or causing an overload

repudiation: denial by one of the entities involved in a communication of having participated in all or part of the communication

forgery: entity fabricates information and claims that such information was received from another entity or sent to another entity

denial of service: prevention of authorized access to resources or the delaying of time critical operations

unauthorized activity: attacker performs activities for which he has no permission or which are in contradiction of an interconnect agreement

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BCSM	Basic Call State Model
CAMEL	Customized Applications for Mobile Enhanced Logic
CCF	Call Control Function
CS1	Capability Set 1
CS2	Capability Set 2
CS3	Capability Set 3
DP	Detection Point
IN	Intelligent Network
INAP	Intelligent Network Application Part
ITU	International Telecommunications Union
PSTN	Public Switched Telecommunications Network
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SRF	Specialized Resource Function
SSCP	Service Switching Control Point
SSF	Service Switching Function
SSP	Service Switching Point
TCAP	Transaction Capabilities Application Part
TDP-R	Trigger Detection Point - Request

4 Functionality

4.1 SSF

The SSF is the Service Switching (SS) function, which, associated with the CCF, provides the set of functions required for interaction between the CCF and a service control function (SCF). It:

a) extends the logic of the CCF to include recognition of service control triggers and to interact with the SCF;

b) manages signalling between the CCF and the SCF;

c) modifies call/connection processing functions (in the CCF) as required to process requests for IN provided service usage under the control of the SCF (ITU-T Recommendation Q.1228 [1]).

4.2 SCF

The SCF is a function that commands call control functions in the processing of IN provided and/or custom service requests. The SCF may interact with other functional entities to access additional logic or to obtain information (service or user data) required to process a call/service logic instance. It:

a) interfaces and interacts with service switching function/call control function, Specialized Resource function (SRF) and Service Data Function (SDF) functional entities;

b) contains the logic and processing capability required to handle IN provided service attempts (ITU-T Recommendation Q.1228 [1]).

4.3 SSF-SCF Interconnection

General (ITU-T Recommendation Q.1228 [1]):

- a relationship between the SCF and SSF is established either as a result of the SSF sending a request for instruction to the SCF, or at the request of the SCF for initiation of a call or for some non call-related reason;
- a relationship between a SCF and a SSF is normally terminated at the request of the SCF. The SSF may also terminate the relationship (e.g. in error cases);
- for IN CS-1, a single SCF may have concurrent relationships with multiple SSFs. A single SSF may only have a relationship with one SCF at a time for any given call. Note that this refers to control as opposed to monitor relationships;
- when the SSF receives call-related IEs from the SCF, it substitutes these IEs for the corresponding call information, and retains all other call information. This applies to ALL call processing-related messages;
- SSF - SCF interconnection could be used to enable operators to use other operators' IN platform. Because SSF - SCF interconnection may also be allowed to service providers with limited resources, security is of paramount interest regarding the availability demands of the SSF service.

Figure 1 shows an internetworking scenario SCF-SCF and SCF - SSF based on the CAMEL Phase 1 Operations. In practice it is necessary to add security facilities to each SCF and SSF involved in the inter-domain communication.

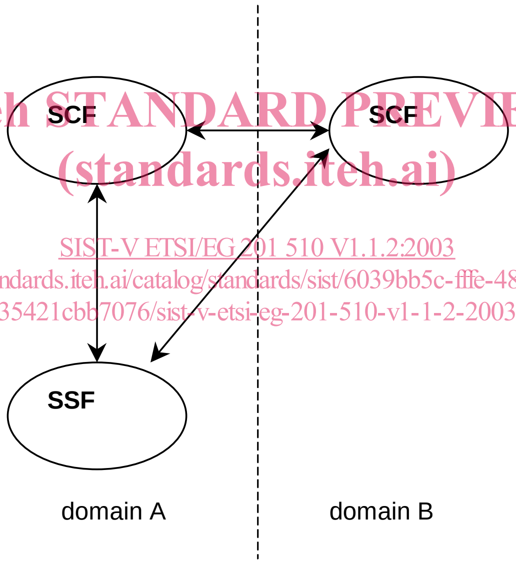

Figure 1: SCF - SSF Interconnection

Because security is important when allowing other operators to connect to an SSF it is necessary to limit the number of operations allowed on the SSF. As a starting point we have taken the CAMEL phase 1 subset of CS-1 minus the MAP operations, which are not applicable to this PSTN model. This results in the following subset of CS-1 operations.

Table 1: CS-1 operations between SSF and SCF

No.	CS-1 operation	Direction
1	InitialDP	SSF -> SCF
2	Connect	SCF -> SSF
3	ReleaseCall	SCF -> SSF
4	EventReportBCSM	SSF -> SCF
5	RequestReportBCSMEvent	SCF -> SSF
6	Continue	SCF -> SSF
7	ActivityTest	SCF -> SSF

Next, a short description will be provided of each operation, together with the parameters and possible security remarks.