

O S C A R

Open & Secure Control of Access & Rights

for

Broadcast Networks

Switched Networks

In the context of the Belgian project

T I T A N

MO.SOC 94.110 V2c
DD 940520

Prep. by G. Maréchal
Philips-SOC
R&D Manager Telecom
Brussels
Tel: +32 2 5256356
Fax: +32 2 5256600

GENERAL PROPERTIES

Control of access
Control of rights

Designed for Broadcast Networks
Usable on Switched Networks

MPEG2 and ATM compatible

Usable for Consumer applications and for Professional ones

Open System :

- Each party can play several roles

- Each party can play his own role in the context of :
 - His rights
 - The rights of the other parties
 - The agreements made between parties

- Each party can control his own key management

- The structure of control is constructed at initialization time
 - From : Full Open
 - To : Pure hierarchical

- Escrow & private policies are possible

- Tokens (f.i. smart cards) can be personalized or anonymous

- Openendedness through the architecture (Specials on project base)

- Many Service Providers in the same smart card

- Many Services per Service Provider

- Reliable cryptographic approach because based on :
 - Public key cryptography for professional applications
 - Separation of key management between authorities
 - Secret and private keys could never leave Tamper Resistant Devices
 - Activations occur within the Smart Cards

- Performance fitting with requirements

SYSTEM

Access Control

Independent Roles

- Copyright Owner CO
- Service Producer SPd
- Service Provider [sometimes called also Service Operator] SPv
- Carrier [sometimes called also Network Operator] CR
- Supplier of equipment/System SS
- User [can be a Physical Person (PP), a Moral Person (MP), an Equipment (EQ)]
- Public Authorities PA
- Terminal Owner TO
- Trusted Third Party TTP
- Issuer ISS

Identified Resources

- Terminal adapter / Terminal
- Server
- Switched Network
- Broadcast Network

Tokens

- Document
- Pocket Computer
- Smart Card

Mechanisms

- Knows (Password)
- Has (token)
- Is (Biometric)

Invoices & Billing Centers

PRINCIPLES

Any party has an authentication token

- Distinguished name
- Pair of Cryptographic keys (Private & Public)

Parties are Authorities (CO, SPd, SPv, CR, SS, PA, TTP, ISS)
Users (Physical Person, Moral Person, Equipment, Anonymous token holder)
Groups

Public Keys and Private Keys are handled according to the EEC "*Greenbook of Information Security Systems*" i.e.

Identity Registration
Key Generation
Key Certification
Key Validation
Directory of certificates & Blacklists

Associations between parties are reflected in the tokens under the control of their Issuer

Commitment of parties w.r. services/programs are digitally signed

f.i. Subscription from <date> to <date>

Activation of rights occurs only after authenticity, integrity control and deciphering, in the context applicable

The operations are organized by allocating roles to parties.



