FIGURE 1

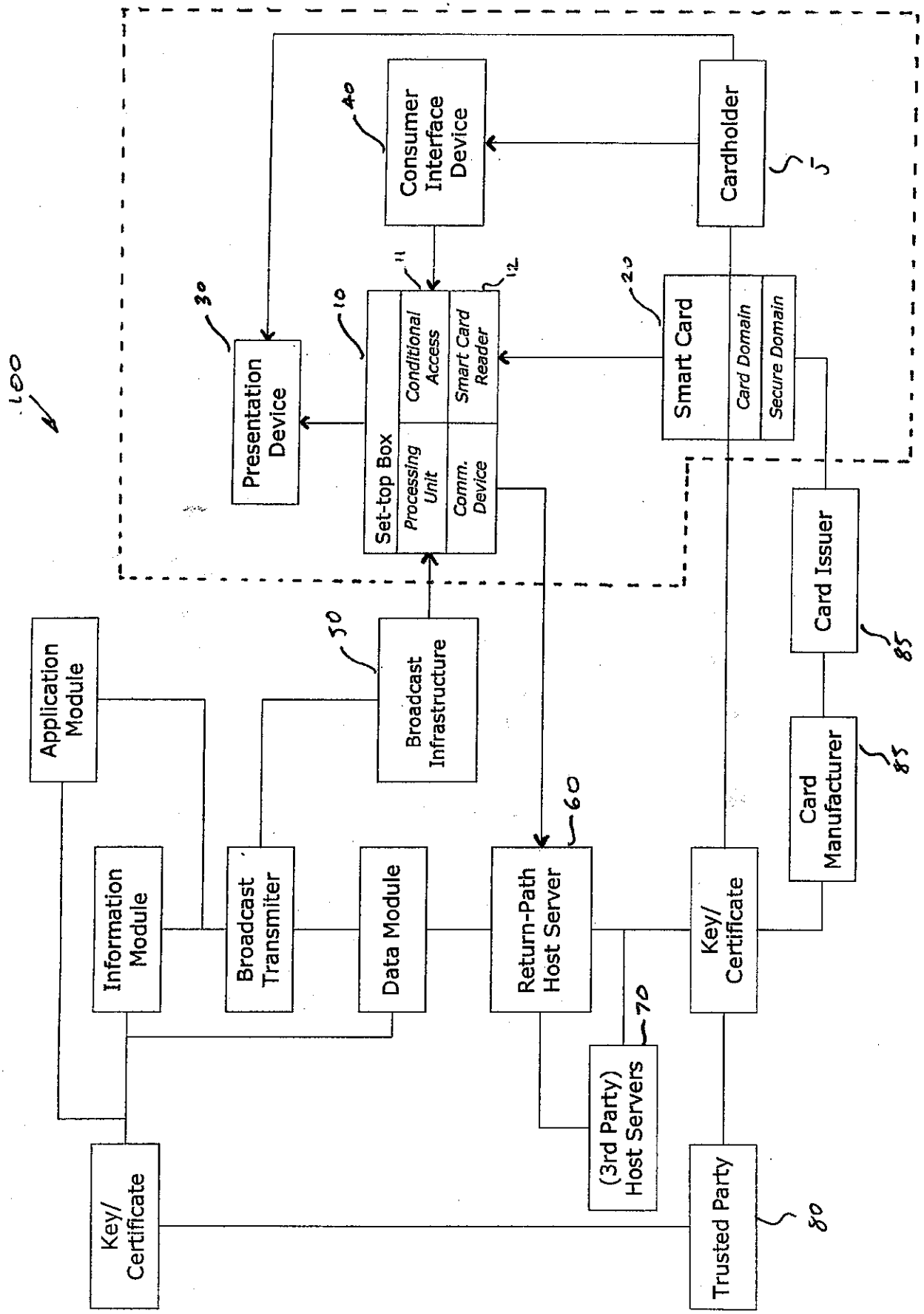

100
Consumer Interface Device
40
Cardholder
J
Presentation Device
30
Set-top Box
10
Processing Unit
Comm. Device
Conditional Access
Smart Card Reader
11
12
Smart Card
20
Card Domain
Secure Domain
Application Module
Broadcast Infrastructure
50
Card Issuer
85
Information Module
Broadcast Transmiter
Data Module
Return-Path Host Server
60
Key/ Certificate
Card Manufacturer
85
(3rd Party) Host Servers
70
Key/ Certificate
Trusted Party
80

FIGURE 2

Secure Access Matrix

Security Levels			System Components			
			Broadcast Infrastructure (50)	Set-Top Box (10)	Return-Path Host Server (60)	Smart Card (20)
200	1	Physical Access, via Conditional Access entitlement	Specifies who is entitled to **physically access** the Set-Top Box to perform secure interactive TV services.	NA	NA	NA
201	2	*Above* <u>*PLUS*</u> Application Access via Conditional Access entitlement	**Application Selection**: Specifies which Set-Top Box's secure interactive TV application/services can the cardholder have access to, given their physical access.		NA	NA
202	3	*Above* <u>*PLUS*</u> Return-Path Server authentication	**Authentication** can be done through (1) decentralised processing, whereby key pairs are transmitted from Return-Path Host Server to Set-Top Box for on-board processing on the Set-Top Box, or (2) centralised processing whereby the Return-Path Host Server's secure module does the Set-Top Box authentication centrally, via secure communications infrastructure, and working in combination with the Set-Top Box's Conditional Access security module. Using *Free-Read-Write* smart card access.			NA
203	4	*Above* <u>*PLUS*</u> Smart Card authentication	**Key Management Selection**: Key pairs and APDU commands on the Smart Card interact, in combination or separately, with (1) Broadcast Infrastructure, and/or (2) Set-Top Box, and/or (3) Return-Path Host Server.			
204	5	*Above* <u>*PLUS*</u> Pre-registration, without PIN	**Transaction Verification**: The secure interactive TV services are verified against the Cardholder's pre-registered information (entitlement), which is stored on a centralised host server.			
205	6	*Above* <u>*PLUS*</u> PIN/ Biometrics	**Cardholder Verification**: Specific verification of cardholder identify is carried out prior to completion of the secure interactive TV services.			