PowerKey™ Conditional Access System Phase 1.0

System Overview

Revision 1.0

NOTICE OF DISCLAIMER

This interface definition / system overview is published by Scientific-Atlanta, Inc. (S-A) to inform the industry of the requirements and operational characteristics for interaction with the S-A Digital Broadband Delivery System for the delivery of broadcast and / or interactive video services.

S-A reserves the right to revise this document at any time for any reason, including but not limited to, conformity with standards promulgated by various agencies or industry associations, utilization of advances in the state of the technical arts, or the reflection of changes in the design of any equipment, techniques, or procedures described or referred to herein.

S-A makes no representation or warranty, express or implied, of any kind with respect to this document or the any of the information contained herein. YOUR USE OF OR RELIANCE UPON THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS AT YOUR OWN RISK. S-A shall not be liable to you for any damage or injury incurred by any person arising out of the your use of these materials.

This document is not to be construed as conferring by implication, estoppel or otherwise any license or right under any copyright or patent whether or not the use of any information in this document necessarily employs an invention claimed in any existing or later issued patent.

Table of Contents

1.0 PowerKEY™ Conditional Access System

Historically, the primary need for Conditional Access (CA) systems on broadband networks has been to protect against signal theft. With the advent of digital compression and two-way services, the range of security issues and those affected is increasing dramatically.

For example, interactive networks that exchange private data (such as credit card numbers) must allow for selective access to services based on validated authorization. Ensuring the confidentiality of subscriber information, such as service or product orders, will be a critical requirement for electronic commerce. In addition to network operators, content owners, service providers, billing providers, and end users also have security concerns; inadequate security is a barrier to the growth of digital broadband networks. Therefore network operators must have a sophisticated security system to provide services such as:

- digital pay-per-view / premium channels / video-on-demand
- high speed data communications
- interactive communications
- electronic shopping

Scientific-Atlanta created the PowerKEY™ CA system specifically to address this growing list of new concerns as well as the traditional need to protect against signal theft.

In contrast to other CA systems that employ only private key methods, the PowerKEY™ CA system employs private *and public key* methods. The advantage of the public key approach is greater security for the subscriber, and for service provider messaging. It also provides a simpler way to enable multiple content owners within a single network. Public key methods are described in more detail in Section 1.2.1.

Other advantages and unique features of the PowerKEY™ CA system include:

- supports a wide variety of networks including CATV broadcast, data, broadband, switched, MMDS, FTTC / SDV, and satellite. PowerKEY™ CA system is transparent to any network type
- employs RSA algorithms using mathematically matched pairs of keys for encryption and decryption; many consider this to be standard for public key-private key cryptography
- enables many classes of applications, including video and data access
- supports global standards; PowerKEY™ CA is the industry's first licensable, open CA system that supports global standards
- supports multiple content providers

- implements all critical elements, including key generation, encryption / decryption, digital signature, authentication, and physical security

1.2 Overview of Encryption/Decryption Techniques

With the integration of the Scientific-Atlanta system design, RSA Data Security protocols, Cylink protocols, and other leading cryptographic methods, the PowerKEY™ system design has evolved to an industry leading, technologically advanced security system.

The PowerKEY™ CA system provides different service and key management layers, and uses different encryption techniques to obtain optimized performance. Public / private key techniques are used in certain layers of this system and secret key techniques are used in others to achieve the highest level of security, reliability and flexibility possible.

1.2.1 Public/Private vs Private Cryptography

Two types of key mechanisms are possible in cryptography systems:

- public / private key
- secret key

Scientific-Atlanta's PowerKEY™ CA system is the broadband industry's *first* CA system to support *both* public key and secret key cryptography.

The secret key only approach utilizes *one* key for both the encryption and decryption process. To send information to a subscriber, a content provider needs the subscriber's secret key, and the subscriber needs the *same key* to decrypt the received information. Since the key is used to both encrypt and decrypt the content information, maintaining the secret key's security is vital. Secret keys are stored in both the subscriber's set-top unit and the network. To allow content providers to send encrypted data to a subscriber they must access the secret key. This means the secret key must be transported to the provider. As a result, within this mechanism, several potential points of failure exist.

Public key systems use a mathematically matched pair of keys for encryption and decryption: a public key to encrypt content data and a private key to decrypt the data. The public key cannot be used to decrypt data it encrypts. Additionally, only the intended recipient, the holder of the matched private key, is able to decrypt the message. Since the public key cannot be used to decrypt transmitted content, this approach poses a significantly *lower security risk* than a private or secret key. Additionally, public keys can be stored in the network, and access can be offered only to content providers.

Compared to secret key only encryption, the number of potential severe points of failure in this system is reduced to one: the secrecy of the matched private key in the subscriber's set-top unit. Mathematically, to discover the private key would require

the factoring of a very large number (greater than 230 digits long) into its two prime factors. To obtain a single RSA private key, the best known factoring algorithms would take thousands of years with current state-of-the-art computers.

1.2.2 Message Authentication

Through the authentication of transported messages, the PowerKEY™ system can be used to guarantee that the data being transmitted to or from a subscriber's set-top unit has not been altered. This would included un-intended, third party manipulation of data or, in the case of computer file transmission, the infection of viruses within the data.

The ability to digitally sign data transmitted through the PowerKEY™ system is another benefit. This feature provides a mechanism for authenticating the acceptance and transmission of information. Through this feature, a content provider can be assured that a particular subscriber's set-top unit was used to request a movie or purchase an item. Conversely, when a subscriber receives confirmation messages from a provider, they can be assured that the provider was the actual organization sending the confirmation. Each of these are achieved through PoweKEY's ability to provide message authentication through digitally signing a unique identifier to each entity transmitting information through the system.

1.3 PowerKEY™ Operation

From the end-user's perspective, the PowerKEY™ CA system is nearly invisible, working in the background. The set-top unit may require a smart card or PCMCIA depending upon how the network operator chooses to implement PowerKEY™. Otherwise the end-user merely uses the set-top unit and its applications.

From the network operator's perspective, PowerKEY™ can be smoothly migrated into the Scientific-Atlanta Digital Broadband Media System.

The key equipment and software requirements are indicated below:

- PowerKEY™ Encryption Cards, which may be housed in a Scientific-Atlanta MPEG-2 Encoder or Broadband Integrated Gateway, to encrypt MPEG audio, video and data
- Transaction Encryption Devices to encrypt Entitlement Management Messages (EMM)
- DNCS: PowerKEY Security Control System software to manage keys, provide an X.509 public key certificate repository, and control the Scientific-Atlanta PowerKEY™ Conditional Access System

The set-top unit requires:

- a DES (or DVB Superscrambling) decryption device
- a secure microprocessor embedded with PowerKEY™ software

Three alternatives exist for placement of these components:

- within the set-top unit itself
- in an ISO 7816 smart card
- in a DVB compatible PCMCIA Card

1.4 Standards and Openness in PowerKEY™

Standards reduce the risk of obsolescence and allow interoperability between dissimilar products. Scientific-Atlanta's consistent adherence to standards is evident in the PowerKEY™ system. PowerKEY™ CA system is designed to be compatible with global open standards, such as MPEG, DVB and DAVIC. PowerKEY™ is fully MPEG-2 transport compliant. Additionally, a version that is DVB compliant through the use of the Superscrambling algorithm and other DVB specifications is available.

The use of RSA's encryption methods also supports this adherence to standards. RSA is currently used in a wide variety of products, platforms and industries around the world, and is part of many official standards. Furthermore, RSA has existed for many years, and has successfully withstood substantial sophisticated attacks utilizing state-of-the-art computing facilities and techniques.

In addition, Scientific-Atlanta has announced its policy to license the PowerKEY™ CA system to other manufacturers of receiving devices such as set-top units. This ensures a *truly* open strategy.

1.5 Licensing

Scientific-Atlanta is licensing the PowerKEY™ CA system to other manufacturers to allow network operators a wide range of sources of supply of set-tops on a competitive basis.

1.6 Conclusion

The PowerKEY™ system design is based on the most thorough and proven digital security systems as well as Scientific-Atlanta's more than 15 years of experience in the conditional access market. Designed to meet today's digital security demands and evolving digital requirements, the PowerKEY™ CA system can be used now and in the future as the market continues to evolve. With support for leading international standards, this system is poised to meet forthcoming interoperability demands.

Additionally, whether PowerKEY™ is purchased directly from Scientific-Atlanta or through a technology license, the system is ready to meet the demands the digital market has to offer.