



NDS Americas, Inc.  
3501 Jamboree Rd.  
Suite 200  
Newport Beach, CA 92660  
Phone: (949) 725-2500  
Fax: (949) 725-2505

January 14, 2003

VIA FACSIMILE 703 305 8885  
One of Eight Pages

United States Patent and Trademark Office  
Office of Legislative and International Affairs  
Room 902  
2121 Crystal Drive  
Arlington, VA 22202

Attn: Velica Steadman

RE: Comments on the TEACH Act Study on Technological Protection Systems

Please find enclosed comments from NDS pursuant to the TEACH Act Study on Technological Protection Systems.

We appreciate the opportunity to offer these comments and welcome further participation on the Study.

Thank you.

A handwritten signature in black ink, appearing to read "E. J. Burakowski".

Edward J. Burakowski  
NDS Americas, Inc.

Enclosure

## **Contents**

<b>OVERVIEW .....</b>	<b>3</b>
<b>TECHNOLOGICAL PROTECTION SYSTEMS DEVELOPED BY NDS .....</b>	<b>3</b>
PATENT: SECURE DOCUMENT ACCESS SYSTEM .....	3
PATENT: NON-STANDARD CODING SYSTEM .....	4
PATENT: DIGITAL CONTENT DELIVERY SYSTEM AND METHOD .....	5
PRODUCT: VIDEOGUARD® .....	6
<b>SYSTEMS DEVELOPED THROUGH AN OPEN CONSENSUS PROCESS.....</b>	<b>6</b>
PRODUCT: SECURE VIDEO PROCESSOR.....	6
<b>CONCLUSION .....</b>	<b>7</b>

## OVERVIEW

---

This document contains NDS's comments related to the TEACH Act study on technological protection systems developed to protect digitized copyrighted works and prevent infringement.

NDS is a premiere provider of security solutions for satellite, terrestrial, and cable television. We have assisted dozens of customers in providing security solutions for millions of deployed digital receivers around the world. Due to our years of expertise in the content security field, our customers are asking us to identify technologies that will further protect their valuable digital assets as they are distributed to homes and secure networks around the globe.

Through our relationships and discussions with the Motion Picture Association (MPA), studios, CE manufacturers, and broadcasters, we have been made acutely aware of the concerns with the possible theft and misuse of digital content.

## TECHNOLOGICAL PROTECTION SYSTEMS DEVELOPED BY NDS

---

NDS has the following patents and products that deal with protecting digitized works. It includes technological protection systems developed by NDS that have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems.

### Patent: Secure Document Access System

*Patent No: US 6,298,441 B1*

*Date of Patent: Oct. 2, 2001*

A method for downloading a document via a communications medium operatively associated with a communications interface, the method including receiving the document from the communications medium, placing an information storage smart card in removable operative association with the communications interface, and conditionally transmitting the document from the communications interface to the information storage smart card and storing the document in the information storage smart card. Other related methods and apparatus are also provided.

The present invention seeks to provide access systems having improved security and flexible applications.

The term "access systems" is used in a broad sense to include systems which allow controlled access to communication apparatus, software programs, restricted areas, such as buildings, terrain and departments in a plant, television, satellite and cable television transmissions, video programs, audio programs, computer data and electronic mail and voice information.

The present invention particularly seeks to provide access systems for use with an electronic book system, in which information is typically loaded into an information-storage medium such as a smart card, typically for viewing in a viewing device. Typically, loading of information into the information storage medium is performed in a first device, while the viewing device typically comprises a separate device, typically a device not capable of loading information into the information storage medium or not connected to an appropriate external source of information.

The term "smart card" is used interchangeably with the term "IC card", and is meant to include any device of whatever external form, whether the form of a card or another form such as a key, having internal structure and characteristics similar to those of an IC card.

## Patent: Non-Standard Coding System

*International Publication Number: WO 02/19529 A2*

*International Publication Date: 7 March 2002*

A method for transforming content from a standard form coded in accordance with a standard coding scheme to content in a non-standard form coded in accordance with a non-standard coding scheme.

The method includes providing content coded in a standard form in accordance with a standard coding scheme, the standard coding scheme including at least one syntax element; and altering the content coded in the standard form in accordance with a non-standard syntax modification scheme, thereby producing content encoded in a non-standard form in accordance with a non-standard coding scheme. Related apparatus and methods are also provided.

The present invention seeks to provide improved apparatus and methods for protecting encoded content.

Throughout the present specification and claims, the term "content", in all of its grammatical forms, is used to refer to digital content of any appropriate kind, including, but not limited to, any one or combination of the following: audio content; video content; and content intended for interpretation or execution by a computer or similar device. It is appreciated that rich digital multimedia content, as described above, is a particular type of content; the term "content", as used throughout the present specification and claims, is not limited to rich digital multimedia content. It is further appreciated that the present invention, in certain preferred embodiments thereof, may be particularly useful when used with rich digital multimedia content.

It is believed that the aim of security mechanisms protecting content should be to make the task of stealing the content at any stage as difficult as possible. It is further believed that protecting non-scrambled encoded content, is an important part of the task of making stealing content as difficult as possible. It is a goal of the present invention, in some preferred embodiments thereof to improve security mechanisms protecting content.

A solution to counter the specific problem of stealing non-scrambled encoded content within the client is for content to never appear in a standard compressed form within a client; this solution is achieved, in preferred embodiments of the present invention, by delivering the content in a non-standard bit stream to a non-standard decoder.

It is believed that even non-standard decoders are subject to hacker attacks through reverse engineering, and that it is virtually impossible to prevent such attacks when applied to software running on open platforms; successful reverse engineering is believed to be only a question of time.

In some preferred embodiments of the present invention, reverse engineering may be thwarted by varying the non-standard decoder every so often.

## Patent: Digital Content Delivery System and Method

*International Publication Number: WO 01/50755 A1*

*International Publication Date: 12 July 2001*

The present invention is of a system and a method for flexible, yet secure distribution of digital content items, optionally with an automatic payment mechanism for purchasing such content.

The present invention supports the distribution of content to end user devices from one or more central distribution points, as in client-server models and variations thereof, and/or peer-to-peer distribution, for example between end user devices. In addition, the present invention also supports distribution models within either of these mechanisms for unitary distribution, to a specified end user device, or broadcast/multicast distribution, to a plurality of end user devices. In any case, in order for the distributed content to be operative, for example to be "played back" or otherwise displayed, the recipient end user device must have been in communication with a network control center at least once before the content can be so displayed. It should be noted that optionally such contact may be performed at the time of manufacture of the end user device.

The network control center then enables the recipient end user device to play back or otherwise display the received content, for example by sending a code or other permission message to the recipient end user device. Optionally, the network control center may require payment to be received before enabling the content for the recipient end user device. Thus, the present invention supports flexible distribution of content according to a number of different distribution models, while still preventing unauthorized play back or other display throughout the lifecycle of the digital content item, and optionally enabling assured payments.

According to preferred embodiments of the present invention, there is provided a combination of secure hardware and software to prevent and/or at least retard unauthorized access or "hacking". In order for access to the distributed content to be controlled, the content itself must be protected, for example by encryption or scrambling. Hereinafter, the term "scrambling" is considered to encompass both encryption, which involves the mathematically determined alteration of content to a form which cannot be read without the proper key, and a simpler form of scrambling, which involves the rearrangement of portions of the content, such that the content is only readable when properly rearranged. By protecting the content itself, the present invention enables the content to be completely portable, and to be distributed freely, while still ensuring that control of access to the content is maintained by a central authority. The security of the content is more preferably provided through several basic rules. First, preferably all digital content is encrypted or otherwise scrambled throughout the system, except when being received by the network control center for distribution to the end user device, and at the last physical point immediately prior to actual physical use (play back or other display of the content) at the end user device. For example, with regard to audio data, that point would be the creation of the analog voltage signal for transmission to the analog amplifiers. The physical construction of the integrated circuits handling the digital content at the end user device is more preferably performed such that decryption or unscrambling of the content is only available at that point and such that "clear" or unscrambled content cannot be transmitted outside of the end user device.

**Product: VideoGuard®**

VideoGuard® is the world's leading conditional access system because it is the most secure solution. VideoGuard solutions ensure the security of all data traveling in both directions, regardless of medium. Some of the product's features include:

- NDS smart cards use custom-designed chips and include unique security algorithms for each customer.
- Algorithm-based key generation ensures maximum security and bandwidth efficiency.
- Entitlement information is securely delivered to subscribers in digitally signed packets.
- A secure return path ensures the privacy and integrity of data transferred between viewers and the headend.
- VideoGuard supports both pre-encrypted and real-time session-level encryption for VOD security.
- Copy protection mechanisms and fingerprinting features help prevent illegal redistribution of content.
- VideoGuard provides persistent protection for content stored locally on PVR set-top boxes and for centrally stored VOD content. It enables new business models for stored content.
- NDS ensures that the business model remains secure with extensive operational security activities.

**SYSTEMS DEVELOPED THROUGH AN OPEN CONSENSUS PROCESS**

---

This section includes a description of systems that have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process.

**Product: Secure Video Processor**

The Secure Video Processor standard can be used to define an approach to content protection. With this approach, content is always "under control" until it reaches the final rendering device.

When content is under control, it is encrypted, and it has a tamper-proof license. All of the handling of the content – from time of encryption to time of decryption and decompression – along with the handling of the license is done within the confines of a single hardware chip that acts as a secure video processor (SVP).

Digital content can move freely, and may reside in many locations from the time it is distributed until the time it is finally rendered. The Secure Video Processor Standard creates a chain of control that provides end-to-end control of content from start of distribution until rendering.

---

NDS Comments on the TEACH Act Study on Technological Protection Systems

---

A standard content protection approach must provide a high level of protection as well as deal with many other issues, such as a controlled authorized domain, broadcast flags, and device revocation. It must also support economies of scale, provide a level playing field for competition and ensure customer satisfaction.

The SVP Standard provides several key benefits:

- An end-to-end solution.
- Persistent content protection.
- Protection independent of the physical layer.
- An open standard, fostering competition.
- Compatibility with existing and future protection methods.
- Compatibility with existing legacy digital and analog devices.

## **CONCLUSION**

---

NDS believes the providers of digital content will not be satisfied until they are assured their assets will be protected from the point of transmission to the point of viewing. It is our intention to continue to provide valuable technologies to the industry to forward this goal.