# Link Protection in DLNA

## Table of Contents

## Change Log

| Name | Description | Date |
|---|---|---|
| Kevin Arruda | Created Initial Document | 01/02/2008 |

# Link Protection in DLNA

## What is Link Protection?

Link Protection is a blanket term that refers to the methods employed to thwart attempts to “steal” data from a data transfer link. For DLNA, usually this means an Ethernet link that media is transferred over from a source to a rendering device. For an Unprotected Link, traffic is sent and received in “cleartext”, which means that anybody who can “see” the network traffic is free to copy and use the data on the link as they see fit.

On a Protected Link, encryption is typically used to take this ability away from those watching network traffic. This makes it possible to transfer media from the content source to a rendering device in a secure manner.

## Why do DLNA Devices need Link Protection?

As previously mentioned, on an Unprotected Link, it is possible for anyone with access to the link to copy and read the data transferred over the link. For DLNA, this means that someone could copy or view media during transport from a source to a rendering device. There are a couple main reasons this may not be desirable under the scope of DLNA.

1.) The content being transferred is what is known as “Premium Content”. This means that it was paid for, and probably licensed. Usually Premium Content carries with it restrictions about how it can be used, e.g. whether it can be copied or not. While the source and sink devices themselves may be able to enforce these restrictions, when the data is transferred over a network link it would be possible to circumvent them without Link Protection by copying or modifying the data directly from the network stream.

2.) The content being transferred is private. For example, you may not want other network users to be able to copy your pictures while you are rendering them on your TV from your Digital Camera.

Link Protection in DLNA is provided mostly to facilitate the secure distribution and enjoyment of Premium and Private Content. It allows content to be securely transferred from a DLNA source device (e.g. a DMS) to a rendering device (e.g. a DMP). It provides a guarantee that only the DLNA devices themselves have access to the media, regardless of who has access to the network link used to transfer it between devices.

## How does Link Protection work within DLNA?

Link Protection is implemented in DLNA using two existing Link Protection technologies for network devices – DTCP-IP and WMDRM-ND. These technologies provide a method to establish a secure channel between a source and sink (rendering) device. Both technologies employ different techniques for authentication and content transfer, but they are fundamentally very similar. Both use a form of authentication based on a cryptographically signed Device Certificate and Revocation List. Both also use the 128-bit version of the Advanced Encryption Standard (AES-128) to encrypt data before transport. This encryption establishes the secure channel necessary for Link Protection.
Using these methods, DLNA devices can authenticate other devices as trusted endpoints, as well as communicate without fear of content misuse or theft. This is an important assertion that is necessary to establish DLNA as a trusted medium for the distribution and playback of Premium and Private Content.

## What does this mean for my device?

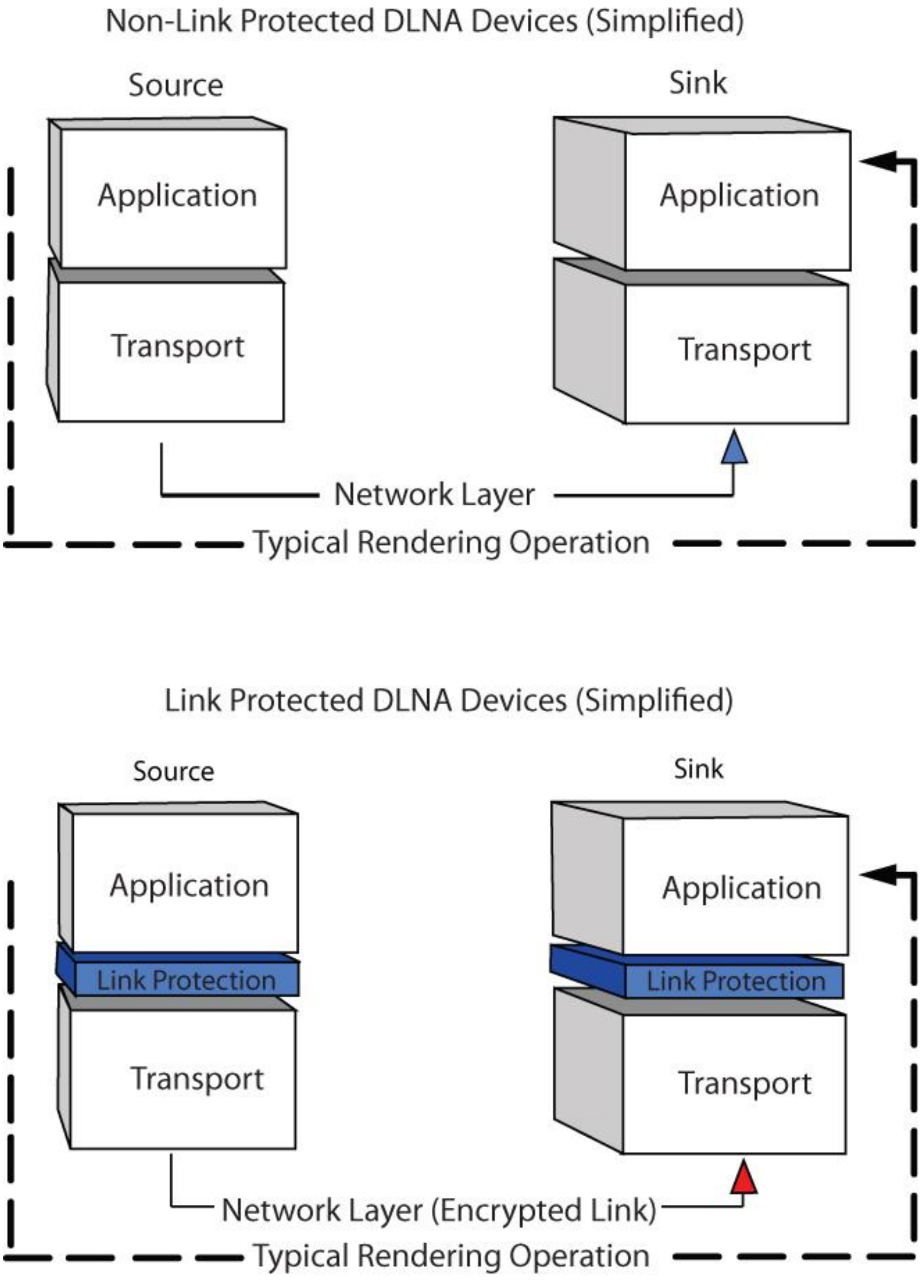
As a device developer, Link Protection can be implemented relatively transparently under an existing device. Most of the elements necessary to implement Link Protection can be inserted as a "shim" between the application and transport layers. For example, when a source receives a request for a media item, the data requested would be passed down through the Link Protection Layer. The Link Protection layer would use the session information established during authentication to encrypt the content data before sending it over the network. In its encrypted form, only the rendering endpoint associated with that session would be able to decrypt the media successfully for rendering. Conveniently, this is exactly the function that the Link Protection layer on the rendering side implements. When content is received over the protected link, the Link Protection layer decrypts it using the relevant session information and passes it up to the Application Layer for rendering.

When implemented in this fashion, the Application Layer sees little difference between content transferred over a Protected vs. an Unprotected Link. A simplified illustration of this concept is shown on the next page.

Link Protection here is presented as a transparent layer between the Application and Transport layers of a DLNA device. In reality, this is not perfectly the case, as there a few other supporting features necessary to make Link Protection work well. Some of these features are defined by the DLNA Link Protection Guidelines, while others come directly from the DTCP-IP and WMDRM-ND Specifications. Included are things like additional metadata elements/attributes, UPnP Services, and Robustness Modifications that DLNA certified Link Protection Devices must implement.

# Link Protection in DLNA

## Illustrative Diagram



Non-Link Protected DLNA Devices (Simplified)
Source
Sink
Application
Transport
Application
Transport
Network Layer
Typical Rendering Operation
Link Protected DLNA Devices (Simplified)
Source
Sink
Application
Link Protection
Transport
Application
Link Protection
Transport
Network Layer (Encrypted Link)
Typical Rendering Operation

Fig 1. Simplified Rendering Flow of Link Protection for DLNA Devices