

# INITIAL TECHNICAL DESCRIPTION OF THE P1817 STANDARD

## Introduction

This document describes a system designed to give consumers perpetual ownership and unrestricted use of copyrighted digital products like video, music, books, and games. The only blocked behavior is that products, which always come with keys, aren't usable without the keys. Consumers will accept this because those who share the keys encounter no restrictions.

This document explains how such a system would work and presents a starting point for the P1817 Working Group. It does not declare how the system *shall* work – that is the job of the Working Group. There are mistakes, inconsistencies, and fatal omissions in this document. The Working Group will resolve them.

## Summary

A Digital Personal Property (DPP) is a single, non-physical, downloadable instance of a copyrighted work, sold to and owned by a consumer, untethered from the vendor and copyright holders, and subject to neither usage nor sharing restrictions for any private use. As consumers expect from a digital product, all of the digital conveniences and advantages consistent with private use are available to the consumer. As is consistent with an open and global standard, all manufacturers of consumer devices and application software are welcome to conform to the DPP standard, enabling device, platform, and vendor independence.

A DPP product item always consist of digital data and a pair of playkeys. Most of the data is encrypted and contained in freely-copiable files. Playkeys are digital objects that consumers can use, share, lend, give and resell, but not duplicate. The playkeys contain the root cryptographic secrets required to decrypt the data. The handling of playkeys is at the heart of how consumer privacy, autonomy, and ownership are preserved.

## P1817 Working Group

The P1817 Working Group will specify the conforming behavior of online playkey banks, device-embedded playkey vaults, content player devices and software, and the manufacturers and distributors of DPP product items.

## Terse Technical Description

- A single DPP *product item* consists of a collection of files in a folder and a maximum of two playkeys – known individually as *twin* playkeys and collectively as a *playkey pair* – one *online playkey* only in a consumer's online playkey bank account and one *device playkey* only in the embedded playkey vault of a consumer device.

- A product item *folder* resides in a user-accessible filesystem. It can be copied without limit and can be stored, manipulated, and used in any storage medium, device, or service.
- A *player* is a consumer device that offers item content access to human users; it protects secrets such as cryptographic keys and unencrypted data from unauthorized discovery.
- The roles of an online playkey bank include: edition registrar, playkey issuer, and playkey host. Typically in a consumer context, a reference to an online playkey bank is a reference to the bank as an playkey host.
  - A *playkey issuer* is the role of an online playkey bank that creates and issues a playkey pair on behalf of a product item vendor. The playkey issuer associates each issued playkey pair with the vendor and may even provide the only enduring link from the consumer's playkey to the vendor.
  - A *edition registrar* is the role of an online playkey bank as a recorder of manifestations (editions) of published works on behalf of a product item publisher. (Each product item is an instance of a particular edition of a work.)
  - A *host registrar* is the role of an online playkey bank as a recorder of playkey hosts, which are primarily device vaults and the consumer devices in which they reside.
  - A *playkey host* is either a consumer *account* in an online playkey bank or a *playkey vault* embedded in a consumer-owned device.
- Playkeys
  - A playkey resides only in a host; it never resides in a user-accessible filesystem.
  - A playkey cannot be copied, but it can be moved freely from one host to another; online playkeys always reside in and move between online playkey bank accounts, and device playkeys always reside in and move between device-embedded playkey vaults.
  - A twin playkey can be used to restore a lost twin playkey or to create a non-existent twin playkey.
  - Each playkey and its twin contain the same reassignable and statistically unique playkey pair identifier, which can be reassigned by a playkey host at the request of any playkey sharer.
- Product items
  - Every product item includes a playkey issuance identifier, which is permanent and globally unique to a playkey pair. A playkey issuer assigns the issuance identifier in a newly-minted playkey on behalf of the vendor.

- Every product item includes a playkey issuer locator, which identifies the playkey bank that minted the playkey.
  - Every product item includes the locators of the online account host and the device vault host.
  - Each product item includes an edition identifier and edition description field, which are permanent values provided by the publisher of the original copyrighted work to the edition registrar. The edition description field is a text string by which a user can recognize the product item.
  - Every product item includes an edition registrar locator, which identifies the edition registrar with which the publisher registered the work edition.
- Passwords
    - Associated with every playkey host is a host owner password ( $PSWD_{HO}$ ), without which the host will not reveal the playkey pair identifiers of the playkeys within it to a player.
    - Associated with every playkey host is a load permission password ( $PSWD_{LP}$ ), without which a player cannot load a playkey into the host.
- Content decryption
    - Each playkey and its twin contain the same statistically unique binding key ( $K_B$ ), which is generated by the playkey issuer and is never modified and never revealed outside of a playkey host.
    - A folder contains a number of files. Within those files are found the encrypted content ( $C_e$ ) and an encrypted content decryption key ( $K_e$ ).
    - Only a playkey host holding the corresponding playkey can decrypt a content decryption key; a player can pass  $K_e$  to the host and receive  $K$  in response. ( $K = \text{decrypt}(K_B, K_e)$ )
    - Having received the content decryption key, a player can decrypt the content and present it to the user of the player. ( $C = \text{decrypt}(K, C_e)$ )
    - A player cannot receive a decrypted content decryption key ( $K$ ) from a playkey host if the information associated with the playkey issuer or edition registrar is detected as corrupted or is missing.
    - Any changes to content or derivations of content are protected by the same playkey pair or set of playkey pairs that protected the original content.
- Players
    - Any player that knows the playkey host locator and the playkey pair identifier can move the playkey away from its current playkey host and into a new playkey host.

- Any player that knows the playkey host locator and the playkey pair identifier can cause the vault to assign a new playkey pair identifier and return the new identifier to the player
- Any player may reveal a playkey locator to any other player.
- Any player may reveal folder locators, or transmit copies of product item folders, to any other player.
- Playkey hosts
  - Playkey hosts communicate as necessary with each other to detect counterfeited playkeys, which have invalid, duplicate, or not-yet-assigned playkey issuance identifiers.
  - Playkey hosts inquire as needed of the playkey issuer as to whether the issuance identifier of its playkey is valid and has been issued to a playkey pair.
  - Device vaults contact corresponding online accounts, and vice versa, whenever a change occurs to a playkey, in order to update the twin playkey with changes.
- Security levels and thresholds
  - Every player and playkey host is assigned a security level, which is a numerical representation of the effort required to compromise its security.
  - Every product item is assigned a security threshold by its playkey issuer. The security threshold is recorded in its playkeys.
  - A playkey cannot reside in a host whose security level is less than that of the playkey.
  - A host cannot deliver a decrypted content key (K) to a player whose security level is less than the security threshold of the associated playkey.

## Detailed Description

### Product Item

A product item is an electronically downloadable, sellable, and consumer-ownable instance of a copyrighted work. It is the thing a consumer purchases and owns. It consists of data objects (e.g., files in a folder) and a playkey.

What's this about? In the physical world you buy one hard-to-clone car and with it comes a couple of easy-to-clone car keys. In the digital world you buy one easy-to-clone folder full of data and with it comes a pair of hard-to-clone playkeys. In the digital realm its easier and more consumer-convenient to keep the tiny keys singular than to try to keep the (often humongous) data set singular.

### Folder

The files may be organized into directories or folders, or it may be delivered and/or stored as a single archive file, but we will simply refer to all of the data that does not

reside in a playkey as being held within a product item folder. We may call it the “product folder”, the “item folder”, or simply “the folder”. We refer to one inclusive folder even though there may be many, and we avoid calling out specific files for now.

### **Playkey**

The playkey is a data object, far smaller than the product item folder. It is called an object and not a file because it doesn’t reside within any filesystem that the user can access. Just as a consumer owns the money in his checking account but can’t manipulate the balance at will, the consumer owns the playkey but has only limited opportunity to examine or modify the data within it.

### **Playkey Pairs**

Playkeys always come in pairs, unless the consumer loses or explicitly chooses to discard one of them. The device playkey exists so that the consumer can operate in complete autonomy and privacy, without any requirement to be tethered to a “big brother”. The online playkey exists for two reasons: (1) so that the consumer can have global access to his property, simply by establishing an Internet connection from a player device, and (2) to provide robust defense of the singular nature of each sold product item, leaving its control with one owner and his trusted sharers, and assuring quick detection of attempts to sell and circulate counterfeited products.

### **Inside the Folder**

Among other things, the folder contains encrypted content ( $C_e$ ) and an encrypted content key ( $K_e$ ). The content ( $C$ ) is the substance of the product, e.g., the text and illustrations of a book, the images and sound of a video work, etc. The key ( $K$ ) is required in order to decrypt the content ( $C = \text{decrypt}(K, C_e)$ ), but only its encrypted version is found in the folder.

### **Inside the Playkey**

Among other things, the playkey contains a binding key ( $K_B$ ). This is the key used to encrypt the content key in the folder. ( $K_e = \text{encrypt}(K_B, K)$ ) The folder is useless without the playkey because only the playkey can decrypt the content key, and that’s because only the playkey knows the binding key. ( $C = \text{decrypt}(\text{decrypt}(K_B, K_e), C_e)$ )

### **Players**

As with all digital data, the product item is only useful to us humans when we employ a digital device. A player may be a dedicated consumer device or an application running on a more general-purpose computing platform. The most basic function of a player is to:

1. access a product item folder,
2. access a playkey,
3. use the playkey to decrypt the content key,
4. use the content key to decrypt the product content, and

5. present the content to the the human users of the player.

### **Everything is a Player**

In this document the player is a generalized user interface device; it provides all of the electronic means by which a human interacts with a product item. These functions may involve the cataloging and tracking of playkeys and their locations, product item folder storage locations and access information, online playkey bank account and device vault access information, and services that support the sharing and exchange of folders and playkeys with other players.

### **Player Security**

The player must accomplish all of this without revealing the content key or the decrypted content data to any malicious external agent. Of course, DPP products are useless unless something get revealed to a human. We humans generally don't consume ones and zeroes; we prefer visible images, audible sounds, and possibly other sensory human receptor paths. The totality of the system that the consumer uses to enjoy his property may often involve multiple devices, connected by wired or wireless means that also involve data encryption (e.g., HDMI). For our purposes we refer here to that entire system is the *player*.

### **Product Delivery and Usage**

The P1817 standard does not address purchase transactions. The scope of the standard begins with the creation of the playkeys and encrypted content, and its delivery to the customer.

1. The vendor registers an edition (manifestation) of a copyrighted work with an edition registrar.
2. The vendor specially encrypts the content and downloads the product item folder to the customer or his designated storage service.
3. The vendor sends required product information to the playkey issuer of its choice.
4. Playkey bank assigns a permanent playkey issuance identifier and an initial playkey pair identifier ( $ID_{PP}$ ) to the product item, and mints an online playkey using data provided by the vendor.
5. The vendor's playkey issuer delivers a message to the purchasing consumer's player; the message contains information required for the player to receive the online playkey and obtain a corresponding device playkey.
6. The purchaser's player moves the online playkey to the purchaser's online bank account – his online host.
7. The purchaser's player directs his online bank to create a twin playkey in a selected consumer device – the device vault.

### **Secure Sessions**

Whenever sensitive or secret information is being exchanged, those communications are always associated with secure sessions. The communicating parties follow a key agreement protocol, then they use the agreed-upon session key to protect their messages by encrypting them before transmission.

### **Binding to a Singular Object**

The most obvious difference between a DPP product and a plain-file product is that the DPP item is singular – it can't be cloned. That singularity is essential to preserving the right of copyright holders to manufacture and profitably sell instances of their works. Singularity is accomplished by the same basic mechanism that other content protection systems use – they encrypt the content and cryptographically bind the content to a (typically physical) singular object, e.g., a DVD optical disc or a particular computer or a unique (non-physical) user account with a given online service. In this respect, the special characteristic of DPP is that the binding can be changed dynamically by the consumer, simply by moving his singular playkey to a different singular playkey host.

What's this about? Hosts protect playkeys to make sure that they can never be copied and to make sure that they can always be used, moved, and shared.

### **Moving Playkeys**

Actually, playkeys come in pairs: matching copies of the same data reside in both an online host and a consumer device – perhaps a WiFi base station, laptop computer, or mobile phone. The consumer may choose to purchase and use any number of devices capable of hosting playkeys. He also can establish one or more playkey host accounts with online banks of his choosing. For each playkey pair he owns, the consumer can choose in which device and in which online account each twin of his playkey pair is stored. He may choose to delete either twin playkey at any point in time; later he can restore the missing twin using the one that remains. (Vendors can issue multiple playkey pairs with a single product, or to offer additional playkey pairs for later sale.)

### **Copying and Storing Folders**

Product item folders may be stored in any device, on any medium, and within any online storage resource that a user may choose, e.g., a USB flash memory, a computer, a recordable CD or DVD, or an online data storage service. Any of those copies may be used as backups or may be actively played, requiring only that there be a connection between the player and the stored folder that has sufficiently high bandwidth and low latency to meet the player's performance requirements.

### **Format and Encoding Conversion**

If a product item carries the content in a form that is not optimal for a given player device, or if the format is incompatible with the capabilities of the player, then the user may use whatever tool or application is available to generate a new encrypted content file that is bound to the same playkey as the original and that will work with the targeted player. The new content may be stored in its own folder, or it may be added to a folder that also contains the original content.

### **Future-proofing**

Similarly, content may be re-encoded if the user wishes or needs to convert a product item to a new encoding standard. The result may be placed into a new folder or may be joined with other encodings in a single folder.

### **Mortal, Yet Never-aging**

Properly cared for, there is no limit to how long a digital personal property can exist. As long as both playkeys are not lost, the missing playkey may be restored. As long as backup copies are managed and preserved, a lost item folder may be restored. Still, by neglect, ineptitude, deceit or malicious actions they can be lost by their rightful owner or lost from existence.

### **Alternatives to Downloading**

Downloading from the Internet is not the only means to deliver DPP product items to customers. Physical storage media can be used to deliver product item folders. These might be shipped to the customer's door, they might be made available at retail outlets or from automated kiosks, or they could be borrowed copies of the item folders of neighbors or friends. Physical media distribution typically suffers from the disadvantage that many, many customers receive the exact same encryption of the same product; however, given that players are already trusted with the content decryption keys, it is quite reasonable to allow player device applications to decrypt, then re-encrypt content for the purchaser, who only needs to employ online transactions to purchase the playkeys for his new purchased property.

### **Playkey Banking System**

Online playkey banks serve in four roles: for consumers they provide *playkey bank accounts* and *host* (e.g., device vault) *registrars*, for vendors they serve as *playkey issuers*, and for publishers and copyright holders that serve as *edition registrars*. These banks are, or are part of, for-profit businesses, and they, together with consumer device and application suppliers, provide the great bulk of infrastructure support for DPP. They may charge for their services, or they may provide their services free of charge as an enhancing component of some ongoing relationship with their customers. It should be unnecessary for the IEEE or other standards bodies to play a major and ongoing role in the maintenance and support of the DPP ecosystem.

The Working Group will need to determine whether or not the same business entity may serve as the registrar, issuer, and bank for a given playkey pair.

### **Playkey Hosts**

Consumers establish playkey bank accounts for their online playkeys. Those accounts are the playkey hosts that protect the consumer-private possession of playkeys, provide internet access to them, and maintain synchronization between their online playkeys and their device playkey twins.

Consumers purchase and own devices that act as catalogers, managers, and players of their digital property. Any of those devices may host a playkey vault, which is a consumer-local and tamper-resistant repository for device playkeys. Devices other

than players may also provide vaults, e.g., a USB flash memory stick or a WiFi basestation.

From the perspective of the consumer, the roles of online playkey accounts and device-embedded playkey vaults are generally equivalent, providing the same product item access and exchange services. Both accounts and vaults are playkey hosts.

#### **Playkey Issuers**

Vendors invoke the aid of their chosen playkey issuers to create playkey pairs and to deliver them to a consumer's online account and device vault. Playkey issuers provide a vendor- and publisher-independent means to verify the authenticity of playkeys. A playkey holder may query the issuer as required to discover if a playkey is valid.

#### **Edition Registrars**

Content publishers register each distinct publishable manifestation of a copyrighted work with an edition registrar of their choice. Edition registrars provide a publisher-independent means to verify the authenticity of the presented title of a product item, and an assured means for consumers to obtain contact information for the publisher.

#### **Host Registrars**

Playkey hosts (primarily device vaults) are subject to loss by being misplaced, damaged, destroyed, stolen, etc. In order to facilitate the restoration of playkeys resulting from the loss of the host, it is valuable to have a single party with which a lost host can be so declared, thus making all corresponding twin playkeys eligible for use in their restoration in a new host.

If the original host reappears and makes contact with the online banking system, it is immediately reset, all of its stored playkeys are erased, and it assumes a new, statistically unique identity.

#### **Default Unidirectional Links**

A consumer can discover and make contact with the vendor or publisher, the issuer, and the registrar because his product item includes information sufficient to identify and locate them. To preserve consumer privacy and autonomy, the ability of a vendor or publisher to locate the host of an online playkey should be highly limited by default, probably to court-ordered examination of transaction records of playkey issuers and work registrars.

#### **Voluntary Bidirectional Links**

Vendors and publishers are welcome to make voluntary vendor and publisher relationships available to consumers, e.g., in exchange for discounts on upgrades or future purchases or for services such as item folder storage or backup. Voluntary links from suppliers to the consumers' playkeys should be severable by autonomous consumer actions such as deleting information from their content item folders or from their playkeys.

### **Counterfeit Handling**

The playkey banking system facilitates the identification of counterfeited playkeys. Playkey pair synchronization occurs, during which the system checks the validity of the playkeys with the issuer and the registrar. There are at least two approaches to handling counterfeits: (1) The consumer's player is notified, after which the user interface always highlights the item as counterfeited, and (2) the consumer's playkey vault is directed to invalidate the device playkey, notify players of its invalid status, and refuse to provide further services for that playkey. The first approach leaves the counterfeit usable, and depends on the social stigma of owning and using forged goods to discourage its further use and encourage reporting of the forgery to vendors and publishers. The second approach prejudices intent and guarantees that the consumer victim pays the price of the illegal activity. Either way, there exists the opportunity for vendors or publishers to offer rewards for information leading to the identification of the counterfeiters.

### **Playkey Hosts**

A playkey host, whether an online bank account or a device-embedded playkey vault, is a secure repository for playkeys. A playkey host can be explained by analogy to a secure room with a number of doors. You knock on a door, present certain information, and receive information in return. What is returned to you depends on the playkeys stored within it. You don't actually get to see or touch the playkeys; the host is the trusted service that lets you utilize the playkey contents.

#### **Item Sharer Doors**

If you want to use a playkey to decrypt a content key, then you must open the "decrypt key" door, identify the playkey of interest, and reveal the encrypted content key. In return you are given the content key, decrypted for you and ready for use to play your product item. The "decrypt key" door enables unrestricted and remote usage and sharing of playkeys without having to move them.

A playkey host has a number of such special-purpose doors (methods). There is a "read playkey" door that will return useful information stored in the playkey, including the title of the work, the rights holders, artists or authors, comments or other annotations that a consumer may have added to the playkey, and other information that identifies the product item. In order to discover this information, all that is needed by the inquirer is to know how to find the right host, knock on its "read" door, and present the unique identifier for the playkey. The "read playkey" method is a principle means by which a sharing player gathers information about titles in a user's or sharer's catalog of available items.

There is also a "transfer playkey" door. If you knock on that door, identify a particular playkey, and also identify a destination host (and a load permission password for the destination), then the source host will respond by locating that destination host, securely loading the playkey to that host, erasing the playkey from itself, and returning to you the new unique identifier by which you can access the moved playkey in its new home. The "transfer playkey" door is the key to trusted sharing, which in turn is the key to inducing consumers to voluntarily limit their property sharing to private, trusted parties. Things disappear when you share with strangers.

A “rename playkey” door enables any sharer to change the playkey pair identifier, without which a player cannot find the playkey even if he accesses the right playkey host.

If content providers are nervous about the efficacy of trusted sharing to limit the scope of real-world product sharing, all they have to do is to build into their products a “return for partial refund” button. The temptation of instant cash ought to provide the required risk, and as a side effect, provide a firm floor to the product’s resale value.

### **Hosts Everywhere**

A playkey isn’t a file; it can’t be stored on a consumer’s filesystem, as on a magnetic or optical disk or in a plain flash memory stick. Playkeys can only reside within playkey hosts; however, hosts will be embedded into a great variety of consumer devices, and there will be a wide selection of playkey banks available to customers in which to host playkeys. For example, commercial banks and internet service providers could provide accounts to their customers to give them playkey storage and access services with online playkey bank accounts. Manufacturers of most any type of digital consumer device could embed playkey vaults into their products, including in computers, in televisions, in cell phones, or in enhanced flash memory sticks.

### **Owning a Host**

For many operations, any party who contacts a host door with a valid unique playkey pair identifier can use the door. Generally, playkey hosts don’t discriminate between clients and will serve whomever comes knocking. Still, a host account or vault is “owned” by one or more particular consumers. They are recognized by the host by presenting a host owner password. Two doors that require the owner password are “list playkeys” and “delete playkey”. If you know the password, then you can request and receive a list of all of the playkey unique identifiers stored in your host, and you can rename, move, or delete any of them that you choose.

### **Sharing a host**

The host owner can share the ability to store playkeys within his host by revealing a load permission password to others. Mom may keep the owner password to herself, but share the load permission password with the kids and their friends, and even Dad. The host owner can choose to share the playkey storage capacity of his account or vault without also enabling all to peruse their entire contents and discover unshared playkeys.

In order to be an untrustworthy sharer you don’t need to own your own host account or vault, you just need to have access to some shared host. Mom may discover that little Billy has borrowed, and failed to return, the music of his friends and left the playkeys in the family account and vault, because Billy doesn’t actually have a playkey host of his own.

### **Playkey Twin Synchronization**

Playkeys typically have twins, one in a consumer device and one in an online account. Each playkey keeps a pointer to its twin, and whenever a change is made to one playkey it contacts its twin so that it can be updated so that they can exchange

information and continue to match each other. It is easy to imagine scenarios where each of two matched playkeys are changed simultaneously during a time when they are unable to contact each other. Those transient mismatches must be reconciled as soon as they again come in contact with each other.

### **Sharing, Lending**

Just as with physical property, DPP can be shared or lent. It is useful for us to distinguish between sharing and lending because they represent two distinct alternatives with respect to DPP, even though we often use the terms interchangeably with physical property. A person *lends* his DPP to another person by facilitating the relocation of a playkey from his playkey host into the host of the borrower. A person *shares* his DPP with another person by empowering that person to use his playkey in place, without moving the playkey to his own playkey host. Sharing is like electronically merging the homes of all sharers into one “virtual home”. Lending is a distinct (if temporary) transfer of the property from a first owner or sharer to a new (temporary) owner.

### **Sharing Playkey URLs**

Any number of players belonging to any number of people can share a single DPP item. This is done by transmitting the playkey URLs to each sharing device, and by either delivering a copy of the item folder to the sharing devices or by sending the URL of an item folder to those devices so that they can stream or copy it as needed.

### **Terminating Sharing**

Any sharer of a product item can either move the playkeys or rename them in place. The actual (socially-defined) owner would typically terminate sharing by contacting either his online account or device vault and changing the playkey pair identifier to a new statistically-random value, thus invalidating the locators of all other sharers without actually moving the playkeys. Of course, any sharer can do the same thing, but the owner of the host account or vault has the additional capability of discovering the new playkey pair identifier by requesting a listing of the stored playkeys; therefore, in order to reliably “take” a product item, the playkeys should be moved to playkey hosts that are shared or owned by the taker and not shared or owned by the giver.

### **Playkey Possession**

Possession of a DPP item is achieved by providing the receiver’s player or other device with a copy or access to a copy of the item folder, and by either moving the playkeys into hosts owned or shared by the receiver or by enabling the receiver to move the playkeys. Any device that shares the DPP item has all of the information required to move its playkeys, and presumably it also has access to an item folder.

### **Playkey Device Loss**

If a device hosting a playkey vault is misplaced, damaged, destroyed, or stolen, then its owner loses access to the playkeys within it. In these cases the online playkey twins can be used to restore the lost playkeys within one or more other devices. Every playkey vault can be reset, erasing all of the playkeys it holds, and receiving a new statistically-unique vault identifier, after which it can be used to store newly-loaded playkeys.

A lost playkey vault is registered with its host registrar as having been lost. The identifier of the lost vault is propagated to all playkey banks. Any contact between that vault and any online bank results in the resetting of the vault and deletion of all of its playkeys. Any attempt to recreate device playkeys from online playkeys requires that the associated bank find the vault identifier on the list of “lost” vaults.

Although it is expected that playkey host losses involve consumer devices and the vaults contained within them, the loss of an online playkey bank (by some catastrophic disaster, business failure, or an act of fraud or sabotage) can also be registered, enabling the use of device playkeys to restore online playkeys.

### **Found Playkey Vault Devices**

Every playkey vault has a unique identifier. Every playkey includes within it the vault identifier for its twin. When an online twin playkey is used to restore a lost playkey, the online host registrar records and identifies the device playkey vault as lost. If the device is subsequently found, the next time that it communicates with an online account to update a twin playkey, it will be reset, all of its playkeys will be erased, and it will receive a new unique playkey identifier. The found vault is perfectly useful, but it is empty.

If the vault-hosting device was stolen, and if the playkeys are removed before the original owner reports it as lost, then the new owner (the crook) gains possession of the stolen DPP items and the legitimate owner loses them. A DPP owner or sharer may protect his property by password-protecting his devices so that a finder cannot remove the playkeys (and folders) before they can be erased.

### **Counterfeiting**

The playkey issuer that created the playkeys on behalf of a content vendor retains only the permanent playkey issuance identifier and the edition identifier, associating that information with the vendor and the publisher. In the case that a consumer should wish to report having received a counterfeit, it may contact the vendor and/or publisher through the playkey issuer and edition registrar.

### **Security Levels**

There are economic reasons why the strength of security and tamper-prevention that is appropriate for a motion picture might be overkill for a song, and music-quality security would likely be inadequate for a movie. To account for this, players and playkey hosts are assigned security levels, and playkeys are assigned security thresholds. A playkey of a given security threshold is not allowed to be held by a playkey host with a lesser security level designation. Similarly, a playkey host will refuse to deliver decrypted content keys to a player whose security level is less than the corresponding playkey’s security threshold.

This allows for very low cost devices to store device playkeys in an inexpensive embedded playkey vault.

### **WOSTS**

Consumers have become accustomed to the concept of self-contained media players that, when tethered to a host product, are adopted by the host and are allowed

to store and play content from that host. These could be called write-only space-time shifters (WOSTS) because they allows consumers to enjoy their content at times and in locations of their choosing, while protecting keys and content by prohibiting them from being read by other devices. Another name for a WOSTS might be an iPod™, which is the name of the device that has set this expectation of behavior solidly into the minds of consumers.

A WOSTS doesn't hold playkeys; instead, a playkey is used by the host device to obtain the content keys, and those content keys are stored in the WOSTS with the appropriately-formatted encrypted content. The WOSTS "forgets" all content and keys from a given host once it begins to receive content from a different host product.

### **Public Fair Use**

Aspects of fair use doctrines that involve the re-publication of part or all of a creative work are not directly compatible with an encryption-based system in which all end use of a creative work remains in the protected, encrypted domain. Extraction of excerpts for news, commentary, critique, parody, etc., all involve judgement calls about the boundaries of fair use and limitations of copyright. Those judgements cannot be made by automated systems, any more than we could replace judges and juries with computers. The options available to the Working Group are (1) to ignore the issue and provide no means for export of content outside of the protection domain, (2) to provide a standard or automated process for delivering requests for such export to some judging body, or (3) to allow the export of protected content while provide a means for registering such export with an export registration authority, so that rightsholders have a means to identify the exporters and the nature of their exports when they feel that an infringement of their rights has occurred.

### **Security Technologies**

The P1817 Working Group will identify symmetric and public key encryption methods, hashes, digital signatures, message authentication codes, key agreement algorithms, etc. These will be chosen in order to protect the integrity of the DPP system, and with the goal of minimizing licensing encumbrances and maximizing openness and vendor- and platform-independence and interoperability.

In general, the smaller the playkeys the better. We may choose to place information into the item folder, rather than in the playkeys themselves. Such items may even include the edition descriptor or locators for the playkey issuer and edition registrar. Some information does not need to be hidden from the consumer, but should nevertheless be protected from tampering or unauthorized modification. A malicious party might, for instance, use a validly-issued playkey for a single song and redirect it for use with premium content such as a feature-length film. This would defeat the ability of the system to automatically detect such a product as a counterfeit because the playkeys would be real and validly issued. However, a consumer's player should present the user with the original title of the product; thus, a consumer would be able to recognize a counterfeit by the mismatch between the valued movie content and the non-matching song title. In other words, a player should refuse to play an item if certain information is corrupted, or better yet, a playkey host should refuse to serve decryption

keys to a player if certain information is corrupted. This is just one example of a myriad of ways in which a security system can be compromised by inadequate design. The Working Group must solicit expertise and leverage broad and open peer review to assure the quality of DPP security.