ÖZET

BİR DİJİTAL HAKLAR YÖNETİM SİSTEMİ (DRM) İÇİN KULLANICI TABANLI İÇERİK ANAHTAR ŞİFRELEME

Dijital medyayı yönetmek için bir yetkilendirilmiş alanı (12) bulunan bir dijital haklar yönetim (DRM) sistemi ve yöntemi olup bir hak yayıncısı gibi yetkilendirilmiş alan veya kuruluş kullanıcı tabanlı içerik anahtarı şifrelemeyi kullanmaktadır. Bir açıdan sistem çok sayıda birbirlerine bağlı cihazı (16) içermekte olup; bir kullanıcı anahtarının (19) yetkilendirilmiş alana ait bir kullanıcıdan belleklenmesi amaçlı bir saklama sistemi, bir içerik anahtarı (32) ile şifrelenmiş içeriği (13) karşıdan yükleme amaçlı bir sistem, bir kullanıcı anahtarıyla şifrelenmiş bir içerik anahtarını karşıdan yükleme amaçlı bir sistem, kullanıcı şifrelenmiş içerik anahtarını kullanıcı anahtarıyla deşifre etme amaçlı bir deşifre sistemi (28) ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir sistem (28) içermektedir.

İSTEMLER

1. Bir DRM tarafından yetkilendirilmiş alan (12) içine dâhil bir dijital haklar yönetim (DRM) cihazı (16A, 16B, 16C) olup DRM cihazı aşağıdakileri içermektedir:

DRM tarafından yetkilendirilmiş alan içindeki diğer cihazlarla veri paylaşma amaçlı bir sistem,

bir kullanıcı yetkilendirilmiş alana katıldığında kullanıcıdan (14A, 14B) bir kullanıcı anahtarını (19) alma amaçlı bir saklama sistemi olup cihaz kullanıcı anahtarını alan içimdeki cihazlarla (16) mübadele etmek ve yetkilendirilmiş alana ait çok sayıda kullanıcının her birinden bir kullanıcı anahtarını belleklemek üzere yapılanmıştır.

bir içerik anahtarı (15) ile şifrelenmiş içeriği (13) alma amaçlı bir sistem,

içerik anahtarını güvenli biçimde alma amaçlı bir sistem,

alınan içerik anahtarını bir kullanıcı anahtarını kullanarak şifreleme amaçlı bir sistem (24); ve

şifrelenmiş içerik anahtarını kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir deşifre sistemi (28).

2. Kullanıcı anahtarının bir akıllı kart içine gömülü olduğu, istem 1'e göre DRM cihazı.

3. İçerik bir içerik sağlayıcıdan (20) indirildiği, istem 1'e göre DRM cihazı.

4. İçerik anahtarının bir hak yayıncısından (18) güvenli biçimde alındığı, istem 1'e göre DRM cihazı.

5. İçerik anahtarını, karşıdan yüklenen içeriğin kullanım haklarını yöneten bir lisans (26) ile güvenli biçimde alındığı, istem 1'e göre DRM cihazı.

6. Yetkilendirilmiş alanın birden fazla birbirine bağlı cihaz (16) içerdiği, istem 1'e göre dijital medyayı yönetme amaçlı bir yetkilendirilmiş alana (12) sahip dijital haklar yönetim (DRM) sistemi.

7. Kullanıcıları temsil eden bir dizi cihaz (14) içerirken kullanıcıları temsil eden cihazlar (14) kullanıcı alana katıldığı zaman kullanıcı ile ilişkili bir kullanıcı anahtarını (19), çok sayıda dijital haklar yönetim cihazı (16) mübadele etmek üzere yapılanmış olduğu, istem 6'ya göre bir dijital haklar yönetim (DRM) sistemi.

8. Bir dizi kullanıcı ve bir dizi birbirlerine bağlı cihazlar (16) arasında dijital medyayı yönetme amaçlı bir yetkilendirilmiş alanı (12) bulunan bir dijital haklar yönetim (DRM) sistemini uygulama amaçlı bir yöntem olup, aşağıdakileri içerir:

yetkilendirilmiş alana ait çok sayıda kullanıcının her birinden, alan içindeki cihazların her birine bir kullanıcı anahtarının sağlanması,

içerik sağlayıcıdan içeriğin (13) yetkilendirilmiş alan içindeki cihazlardan birine yüklenmesi, burada içeriğin bir içerik anahtarı (15) ile şifrelenmesi,

içerik anahtarının (34) hak yayıncısından yetkilendirilmiş alan içindeki cihazlardan birine, güvenli bir kanal üzerinden yüklenmesi,

yüklenen içerik anahtarının yetkilendirilmiş alan içindeki cihazlardan birinde, bir kullanıcı anahtarı kullanılarak şifrelenmesi,

şifrelenmiş içerik anahtarının yetkilendirilmiş alan içindeki cihazlardan birinde, kullanıcı anahtarıyla deşifre edilmesi,

şifrelenmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan birinde, deşifre edilmiş içerik anahtarı ile deşifre edilmesi, ve

deşifre edilmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan birinde kullanılması.

9. Kullanıcı anahtarının bir akıllı kart ve yetkilendirilmiş alana ait bir cihazdan oluşan bir gruptan seçilen bir sistem tarafından cihazlardan her birine sağlandığı, istem 8'e göre yöntem.

10. İçerik anahtarının hak yayıncısından güvenli biçimde alınma aşaması bir lisans yüklenmesini de içerdiği, istem 8'e göre yöntem.

11. Yüklendiğinde ve çalıştırıldığında bir bilgisayar sistemini, İstemler 8 ila 10'a göre yöntemlerden herhangi birini gerçekleştirecek şekilde kontrol eden bir bilgisayar programı.

TARİFNAME

BİR DİJİTAL HAKLAR YÖNETİM SİSTEMİ (DRM) İÇİN KULLANICI TABANLI İÇERİK ANAHTAR ŞİFRELEME

Bu buluş, genel olarak, elektronik içeriği kontrol etmek için Dijital Haklar Yönetimi (DRM) sistemlerine ve daha özel olarak, kullanıcı tabanlı içerik anahtarı şifrelemesini kullanan bir DRM sistemine ilişkindir.

Dijital haklar yönetimi (DRM) dijital medya için telif hakkı korumasına sistematik bir yaklaşımdır. DRM'nin amacı ücretli içeriğin yasadışı dağıtımını önlemektir. Bazı erken DRM ürünleri içeriği belirli aygıtlarla bağlayarak yasadışı içerik dağıtımını sınırlamaya çalışmış olup buna göre içerik yalnızca onaylı bir aygıtta çalınabilmekteydi. Bu yaklaşımdaki sorun; bir kullanıcının, evinin her tarafında veya yakınında bulunan, içeriği oynatmak için kullanılabilecek birden fazla cihazının (örn. bir bilgisayar, DVD oynatıcı, PDA, otomobil vb.) bulunmasıdır. Cihazlar ev içinde kablosuz yönlendiriciler ve diğer teknolojiler aracılığıyla ev içerisinde daha çok birbiriyle bağlantılı hale geldikçe içeriği belirli bir cihaza bağlamak, büyük bir dezavantaj haline gelmektedir.

Bu konuyu ele alan yeni bir yaklaşım, yetkilendirilmiş bir alan kavramını içermektedir. Yetkilendirilmiş alan, kapsamı içinde, içeriğin serbestçe kullanılabildiği kontrollü bir ağı ifade eder. Bununla birlikte içeriğin alan sınırını ihlal etmesi sınırlanır. Böylece alan dahilindeki her cihaz bu alan içinde, içeriğe erişime sahip olmakta ancak alanın dışarısıyla içerik alışverişi katı kurallarla sınırlanmaktadır.

Yetkilendirilmiş alanların uygulanması için ele alınması gereken konulardan biri, alana ait kullanıcılar içeriğe kolayca erişebilirken aynı zamanda içeriğin alan dışına serbestçe yayılmasını önleyecek şekilde içeriğin alana nasıl ulaştırılacağıdır. Bir çözüm, içeriği bir içerik anahtarıyla şifrelemek ve ardından

içerik anahtarını alan içerisindeki cihazlara vermektir. Böyle bir çözümü uygulamak için, içerik anahtarlarını bir alan içindeki cihazlar arasında güvenli biçimde paylaşacak bir sistem gereklidir.

Çeşitli çözümler önerilmiştir. Bir yaklaşımda hakları yayımlayan ile alandaki cihazlar veya cihazların kendileri arasında alışveriş gerçekleştiği zaman içerik anahtarı mübadelesi yapmak için güvenli bir oturum kullanılmaktadır. Bu yaklaşımda içerik anahtarı cihazlarda güvenli bir şekilde saklanmaktadır. Bu sistemin sakıncaları içerik anahtarlarını mübadele etmek için güvenli bir sistem oturumu gerekmesi ve içerik anahtarı belleğinin güvenli olmasının gerekmesidir.

Bir başka yaklaşımda içerik anahtarı bir kullanıcı anahtarı ile şifrelenmekte ve yalnızca bu kullanıcı anahtarına erişime sahip olan cihazlar içerik anahtarını deşifre edebilmektedir. Örneğin OMA (Açık Mobil Platform) tarafından sağlanan bir sistemde Hak Yayımlayıcı her bir alan için tek bir alan anahtarı atamakta ve her bir Hak Yayımlayıcısının kendi alan anahtarlarını atamasına izin verilmektedir. Alan anahtarlarının Hak Yayımlayıcıları arasında paylaşılmaması gerekmektedir. Sonuç genel olarak çok sayıda alan anahtarlarına sahip olmaktır (yani her bir cihaz, lisansları kullanılan Hak Yayımcılarının sayısına eşit miktarda alan anahtarına sahip olmaktadır). Bir Hak Yayımlayıcısı bir içerik anahtarını, içerik anahtarını talep eden alanla ilişkilendirmiş olduğu alan anahtarı ile şifreleyecektir. Bir alana ait cihazlar alan anahtarlarını Hak Yayımcılarından elde edebilmekte ve böylelikle içerik anahtarlarını şifreleyebilmektedir.

SMART-RIGHT ™ tarafından sağlanan benzer bir sistemde, alanın bir alan adı anahtarı vardır ve içerik anahtarı bu alan adı anahtarı ile şifrelenmektedir. Alan adı aygıtları alan adı anahtarını güvenli bir şekilde mübadele etmekte ve her bir aygıt alan adı anahtarını tutmaktadır.

Bu sistemlerin dezavantajları içerik anahtarı yeniden şifrelenmeksizin veya Hak Yayımcısında bir başka arka uç işlemi gerekmeksizin içeriğin bir başka alana

kolayca taşınamaması olgusunu içermektedir.

Bir cihazda içeriğin alınmasını, içeriğin bir içerik anahtarıyla şifrelenmesini, içerik anahtarının bir alan anahtarıyla şifrelenmesini ve şifrelenmiş içerik anahtarı ile şifrelenmiş içeriğin saklanmasını tarif eden, "Kullanım durumuna göre içerik anahtarının koşullu şifrelenmesi esaslı, cihazlar ve alanlar arasında kontrollü içerik kopyalama ve taşıma için sistem ve yöntem" başlıklı US 2003/0076955 belgesine referans yapılmaktadır.

Bir gruba özgü ortak gizli bilgileri tutmak üzere çalışan bir veya daha fazla kayıtlı üye cihazlar içeren bir grup formasyonu / yönetim sistemini tarif eden, "Grup formasyonu/yönetim sistemi, grup yönetim cihazı ve üye cihaz" başlıklı US 2004/0093523 sayılı patent belgesine referans yapılmaktadır.

Buna göre bir DRM ortamında yetkilendirilmiş alanlara içerik anahtarlarını güvenli olarak dağıtmak için bir sistem ve yönteme yönelik ihtiyaç mevcuttur.

Bu buluş bir DRM ortamındaki bir yetkilendirilmiş alan içerisinde kullanıcı tabanlı içerik anahtarı şifrelemeden faydalanma amaçlı bir sistem ve yöntem sunarak, yukarıdakilerin yanı sıra başka sorunları da ele almaktadır. Bir birinci yönü itibarıyla buluş, yetkilendirilmiş alanın; yetkilendirilmiş alana ait bir kullanıcıdan bir kullanıcı anahtarının saklanması amaçlı bir saklama sistemi, bir içerik anahtarıyla şifrelenmiş içeriği karşıdan yüklemek için bir sistem, şifrelenmiş bir içerik anahtarını karşıdan yükleme amaçlı bir sistem ve de şifrelenmiş içeriği kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir sistem içeren birçok sayıda birbirine bağlı cihazları kapsadığı, dijital medyanın yönetilmesi için yetkilendirilmiş bir alanı bulunan bir dijital haklar yönetimi (DRM) sistemine ilişkindir.

İkinci bir açıdan buluş DRM cihazının; DRM'nin yetkilendirdiği alan içindeki

diğer cihazlarla veri paylaşımı amaçlı bir sistem, yetkilendirilmiş alana ait bir kullanıcıdan bir kullanıcı anahtarının alınması amaçlı bir bellek sistemi, bir içerik anahtarıyla şifrelenmiş içeriği alma amaçlı bir sistem, şifrelenmiş bir içerik anahtarını alma amaçlı bir sistem ile şifrelenmiş içerik anahtarını deşifre etme ve deşifre edilmiş içerik anahtarıyla şifrelenmiş içeriği deşifre etme amaçlı bir sistem içerdiği, DRM tarafından yetkilendirilen bir dijital haklar yönetimi (DRM) cihazı sunmaktadır.

Bir üçüncü açıdan buluş; yetkilendirilmiş alandaki cihazların her birine bir kullanıcı anahtarının sağlanması, içeriğin bir içerik anahtarıyla şifrelenip bu içeriğin bir içerik sağlayıcıdan yetkilendirilmiş alan içindeki cihazlardan birine yüklenmesi, içerik anahtarının kullanıcı anahtarıyla şifrelenip bu kullanıcı anahtarının güvenli bir kanal aracılığıyla hak yayımcısına sağlanması, şifrelenmiş içeriğin hak yayıncısından yetkilendirilmiş alan içerisindeki cihazlardan birine yüklenmesi, şifrelenmiş içerik anahtarının kullanıcı anahtarıyla yetkilendirilmiş alan içerisindeki cihazların biri üstünde deşifre edilmesi, şifrelenmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan biri üstünde deşifre edilmesi ve şifrelenmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan biri üstünde kullanılmasını içeren, bir takım kullanıcılar ve birbirine bağlı cihazlar arasında dijital medyanın yönetilmesi amaçlı bir yetkilendirilmiş alanı bulunan bir dijital haklar yönetim (DRM) sisteminin uygulanması amaçlı bir yöntem sunmaktadır.

Dördüncü bir açıdan buluş; yetkilendirilmiş alana ait her bir kullanıcı için bir kullanıcı anahtarını saklama amaçlı bir bellek, bir içerik anahtarıyla şifrelenmiş içeriği karşıdan yükleme amaçlı bir sistem, yetkilendirilmiş alan içindeki bir kullanıcıyla ilişkilendirilmiş bir içerik anahtarının güvenli biçimde karşıdan yüklenmesi amaçlı bir sistem, içeriğin ilişkilendirilmiş kullanıcının kullanıcı anahtarıyla şifrelenmesi amaçlı bir şifreleme sistemi ile şifrelenmiş içerik anahtarını ilişkilendirilmiş kullanıcının kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir deşifre sistemi içeren, yetkilendirilmiş alanın birden fazla sayıda birbirine bağlı cihaz

içerdiği bir yetkilendirilmiş alanı bulunan bir dijital haklar yönetim (DRM) sistemi sunmaktadır.

Beşinci bir açıdan buluş DRM cihazının; DRM'nin yetkilendirdiği alan içindeki diğer cihazlarla veri paylaşımı amaçlı bir sistem, yetkilendirilmiş alana ait bir kullanıcıdan bir kullanıcı anahtarının alınması amaçlı bir bellek sistemi, bir içerik anahtarıyla şifrelenmiş içeriği alma amaçlı bir sistem, bir içerik anahtarını güvenli biçimde alma amaçlı bir sistem, içerik anahtarını ilişkili kullanıcı anahtarıyla şifreleme amaçlı bir sistem ile şifrelenmiş içerik anahtarını kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir sistem içerdiği, DRM tarafından yetkilendirilen bir dijital haklar yönetimi (DRM) cihazı sunmaktadır.

Altıncı bir açıdan buluş; yetkilendirilmiş alandaki cihazların her birine bir kullanıcı anahtarının sağlanması, içeriğin bir içerik anahtarıyla şifrelenip içerik sağlayıcıdan yetkilendirilmiş alan içindeki cihazlardan birine yüklenmesi, içerik anahtarının hak yayıncısından yetkilendirilmiş alan içindeki cihazlardan birine güvenli bir kanal aracılığıyla yüklenmesi, ilişkili kullanıcı anahtarı kullanılarak içerik anahtarının yetkilendirilmiş alan içindeki cihazlardan biri içerisinde şifrelenmesi, yetkilendirilmiş alan içindeki cihazlardan biri içerisindeki şifrelenmiş içerik anahtarının kullanıcı anahtarı ile deşifre edilmesi, yetkilendirilmiş alan içindeki cihazlardan biri içerisindeki şifrelenmiş içeriğin deşifre edilmiş içerik anahtarıyla deşifre edilmesi ve deşifre edilmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan biri üstünde kullanılmasını içeren, bir dizi kullanıcı ve bir dizi birbirine bağlı cihaz arasında dijital medyayı yönetme amaçlı bir yetkilendirilmiş alanı bulunan bir dijital haklar yönetim (DRM) sisteminin uygulanması amaçlı bir yöntem sunmaktadır.

Yedinci bir açıdan buluş; yetkilendirilmiş alanın birden fazla sayıda birbirine bağlı cihazları kapsadığı, bir kullanıcı anahtarının güvenli bir kanal üzerinden hak yayıncısından yüklenerek saklanması amaçlı bir sistem, bir içerik anahtarıyla

şifrelenmiş içeriği karşıdan yükleme amaçlı bir sistem, şifrelenmiş bir içeriği hak yayıncısından yükleme amaçlı bir sistem ile şifrelenmiş içeriği ilişkili kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir deşifre sistemi içeren bir dijital haklar yönetim (DRM) sistemi sunmaktadır.

Bir sekizinci açıdan buluş dijital haklar yönetim (DRM) cihazının; DRM'den yetkilendirilmiş alan içindeki diğer cihazlarla veri paylaşma amaçlı bir sistem, bir kullanıcı anahtarını hak yayıncılarından güvenli bir kanal aracılığıyla yükleyerek saklama amaçlı bir sistem, bir kullanıcı anahtarını bir kullanıcıya güvenli biçimde yükleme amaçlı bir sistem, bir içerik anahtarıyla şifrelenmiş içeriği alma amaçlı bir sistem, kullanıcı anahtarıyla şifrelenmiş bir içerik anahtarını alma amaçlı bir sistem ile şifrelenmiş içerik anahtarını kullanıcı anahtarıyla deşifre etme ve şifrelenmiş içeriği deşifre edilmiş içerik anahtarıyla deşifre etme amaçlı bir deşifre sistemi içerdiği, DRM'nin yetkilendirdiği bir alan içinde kullanılma amaçlı bir dijital haklar yönetim (DRM) cihazı sunmaktadır.

Dokuzuncu bir açıdan buluş, bir kullanıcı anahtarının bir hak yayıncısından güvenli bir kanal üzerinden yetkilendirilmiş alan içindeki en az bir cihaza yüklenmesi, hak yayıncısından gelen kullanıcı anahtarının bir kullanıcıya ait bir akıllı karta yüklenmesi, içeriğin bir içerik anahtarıyla şifrelenip içerik sağlayıcıdan yetkilendirilmiş alan içindeki cihazlardan birine yüklenmesi, içerik anahtarının kullanıcı anahtarıyla şifrelenip, şifrelenmiş içerik anahtarının hak yayıncısından yetkilendirilmiş alan içindeki cihazlardan birine yüklenmesi, şifrelenmiş içerik anahtarının yetkilendirilmiş alan içindeki cihazlardan biri üstünde kullanıcı anahtarıyla deşifre edilmesi, şifrelenmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan biri üstünde deşifre edilmiş içerik anahtarıyla deşifre edilmesi ve deşifre edilmiş içeriğin yetkilendirilmiş alan içindeki cihazlardan biri üstünde kullanılmasını içeren, dijital medyanın bir dizi kullanıcı ve bir dizi birbirine bağlı cihazlar arasında yönetilmesi amaçlı bir yetkilendirilmiş alanı bulunan bir dijital haklar yönetim sisteminin (DRM) uygulanması amaçlı bir

yöntem sunmaktadır. Buluş, bağımsız istemler 1 ve 8'de tarif edilmiştir. Buluşun bu ve diğer özellikleri, ekli çizimlerle bağlantılı olarak ele alınan aşağıda yer alan buluşun çeşitli açılardan ayrıntılı tarifinden daha kolay anlaşılacak olup bu çizimlerden;

Şekil 1 bir yetkilendirilmiş alanı bulunan bir DRM sistemini göstermektedir.

Şekil 2 buluşun bir birinci yapılandırmasına uygun olarak kullanıcı tabanlı içerik anahtarı şifrelemeden yararlanan bir yetkilendirilmiş alanı bulunan bir DRM sistemini göstermektedir.

Şekil 3 buluşun bir ikinci yapılandırmasına uygun olarak kullanıcı tabanlı içerik anahtarı şifrelemesinden yararlanan bir yetkilendirilmiş alanı bulunan bir DRM sistemini göstermektedir.

Şekil 4 buluşun bir üçüncü yapılandırmasına uygun olarak kullanıcı tabanlı içerik anahtarı şifrelemeden yararlanan bir yetkilendirilmiş alanı bulunan bir DRM sistemini göstermektedir.

Buna göre çizimlere bakıldığında Şekil 1, bir DRM sisteminin (10) genel bir görünümünü tasvir etmektedir. DRM sistemi (10) bir yetkilendirilmiş alan (12), bir hak yayıncısı (18) ve bir içerik sağlayıcısı (20) içermektedir. Yetkilendirilmiş bir alan (12) örneğin bir dizi kullanıcıyı (14) (örneğin Kullanıcı (14A), Kullanıcı (14B)) ve bir dizi birbirlerine bağlı cihazları (16) (örneğin (16A), (16B), (16C)) içerebilir. Genel olarak cihazlar (16) bir yere alan ağı, sanal özel ağ, internet, intranet, kablosuz ağ vb. gibi her türden ağ yoluyla birbirlerine bağlıdır. Kullanıcılar (14) kullanıcı kimliğini doğrulayabilen akıllı kartlar veya diğer cihazlarla temsil edilebilir ve cihazlar (16) DRM korumalı içeriği yürüten (örneğin kullanan, çalan, gösteren vb.) DRM etkinleştirmeli cihazları içerebilir. Bir hak yayıncısı (18) genellikle teknikte bilinenler gibi güvenilir bir üçüncü tarafı ifade etmektedir. Bununla birlikte hak yayıncısı (18) tarafından sağlanan işlevler içerik sağlayıcısı (20) tarafından gerçekleştirilebilir. Çalışma sırasında bir kullanıcı DRM korumalı içeriği (C13) elde etmek üzere içerik sağlayıcısıyla (20) temas kurmaktadır. Bir içerik lisansı gibi kullanım hakları (R11) bir hak

yayıncısından (18) elde edilmektedir. İçerik (C13) ve haklar (R11) yetkilendirilmiş alana (12) devredildiğinde kullanıcı, içeriği yürütmek için cihazlardan herhangi birini (16A), (16B), (16C)) kullanabilmektedir. Aşağıda tarif edildiği gibi içerik bir içerik anahtarıyla şifrelenmekte ve içerik anahtarı bir "kullanıcı anahtarı" ile; örnek olarak bir açık anahtar altyapısı, (2) bir simetrik anahtar vb. gibi bir asimetrik anahtar şifrelemede kullanılana benzer bir açık/özel anahtar çiftinin bir (1) açık anahtarı ile şifrelenmektedir. Asimetrik anahtar şifreleme amaçları açısından "kullanıcı anahtarı" şifreleme amaçları yönünden açık anahtarı ve deşifre etme amaçları yönünden de özel anahtarı ifade etmektedir. Buluş, kullanıcı tabanlı içerik anahtarı şifrelemenin uygulanması için çeşitli yapılandırmalar sunmaktadır. Şekil 2, kullanıcı tabanlı içerik anahtarı şifreleme kullanılarak buluşu uygulama amaçlı bir birinci açıklayıcı yapılandırmayı göstermektedir. Bu yapılandırmada alana katılan bir kullanıcıya (örn. Kullanıcı A), örn. alan (12) içindeki cihazların (16) tümüne sağlanan bir akıllı kart içine gömülü bir kullanıcı anahtarı (KA 19) sağlanmaktadır (asimetrik şifreleme durumunda örneğin, yalnızca özel anahtarın mübadele edilmesi gerekecektir). Kullanıcı anahtarı güvenli bir biçimde mübadele edilebilmektedir. Bir hak yayıncısına (18) ayrıca, içerik sağlayıcıdan (20) elde edilmiş bir içerik anahtarını (CK) (15) şifrelemek üzere bir içerik anahtarı (KA) (19) temin edilmektedir. Kullanıcı bir lisans satın aldığında lisans (26) ve şifrelenmiş içerik anahtarını (34) içeren bir dizi haklar (30), alan (12) içindeki bir cihaza gönderilmektedir. Cihazlardan (16) herhangi biri şifrelenmiş içerik anahtarını (34) aldığı zaman anahtar, bir deşifre sistemi (28) tarafından, bir kullanıcı anahtarıyla (KA) (19) şifrelenebilmektedir. Daha sonra şifrelenmiş içerik anahtarı (CK) (15) içerik sağlayıcı (20) tarafından sağlanan şifrelenmiş içeriği (32) deşifre etmek için kullanılabilmektedir.

Örnekleyici bir işlem, aşağıdaki gibi tarif edilmektedir:

1.Kullanıcı A alana (12) katılır. Kullanıcı A'nın akıllı kartı ve alan (12) içindeki cihazlar (16), Kullanıcı A ile ilişkili kullanıcı anahtarını (KA) (19)

güvenli biçimde mübadele eder. Mübadeleden sonra her bir cihaz (16) (KA) (19)'u tutar. Alana (12) yeni katılan bir cihaz, (KA) (19)'un diğer cihazları tarafından veya kullanıcı cihazının (örn. akıllı kart) (14) kendisi tarafından bilgilendirilir.

2.Kullanıcı bir içerik sağlayıcıdaki (20) bir DRM içerik öğesini (C) tarar ve satın alır.

3.Kullanıcı A içerik öğesi (C) için bir hak yayıncısında (18) bulunan bir lisansı tarar ve satın alır.

4.İçerik anahtarı (CK 15) (C öğesini şifrelemek için kullanılan anahtar), içerik sağlayıcı (20) ve hak yayıncısı (18) arasında bir arka uç işlemi ile güvenli biçimde mübadele edilir.

5.Kullanıcı (A) kullanıcı anahtarını (KA 19) hak yayıncısına (18) gönderir. İsteğe bağlı olarak hak yayıncısı (18) kullanıcı anahtarını (KA 19) gelecekte kullanmak için ön belleğe alır.

6.Hak yayıncısı (18) içerik anahtarını (CK 15) (KA 19) $CK_{şifreli,KA}$'ya şifreler. $CK_{şifreli,\ KA}$ = Şifrele (CK, KA)

7.Şifrelenmiş içerik anahtarı $CK_{şifreli}$, KA, Kullanıcı (A)'nın alanındaki (12) cihaza teslim edilir. Kullanıcı (A)'nın alanındaki bir cihaza aynı zamanda lisans da teslim edilir. $CK_{şifreli}$, KA lisans içinde gömülü olabilir veya ayrıca gönderilebilir.

8.İçerik öğesi (C 13) içerik anahtarı (CK 15) ile şifrelenir. $C_{şifreli}$ = Şifrele (C, CK)'ya eşit olup Kullanıcı (A)'nın alanındaki (12) bir cihaza teslim edilir.

9.Alanın bir kullanıcısı şifreli içerik öğesini (C13) yürütme için bir cihaz kullanır. Lisans içerik öğesini (C) kullanma iznini verdikten sonra cihaz (KA 19)'u kullanıp (CK 15)'i üreterek şifrelenmiş içerik anahtarı $CK_{şifreli}$'yi deşifre eder. CK = Deşifre($CK_{şifreli,\ KA}$, KA). Sonrasında cihaz, $C_{şifreli}$ (32) içerik öğesini deşifre etmek için deşifre edilmiş içerik anahtarını (CK 15) kullanır. C = Deşifre ($C_{şifreli}$, CK) eşitliği gerçekleştikten sonra cihaz içerik öğesini (C 13) kullanabilir (oynatabilir, yürütebilir vb.).

Benzer bir senaryo Kullanıcı (A), (B) ile değiştirilerek ve (KA) (KB) ile

değiştirilerek Kullanıcı (B) içinde mümkündür. Alan içindeki her bir cihaz (12) hem Kullanıcı (A)'nın hem de (B)'nin kullanıcı anahtarını bulundurduğundan her bir cihaz her iki kullanıcının da içeriğini kullanabilmektedir.

Kullanıcı tabanlı bir içerik anahtarı şifreleme sisteminin bir ikinci yapılandırması Şekil 3'te tasvir edilmektedir. Bu yapılandırmada her bir kullanıcının (Kullanıcı (A), Kullanıcı (B)) bir adet anahtarı (örneğin Kullanıcı (A) için (KA 19), Kullanıcı (B) için (KB 21)) bulunmaktadır ancak hak yayıncısı/yayıncıları (18) kullanıcı anahtarlarını bilmemektedir. Kullanıcı anahtarları yalnızca alan (12) adı ile bilinmektedir. Bu nedenle hak yayıncısı (18) teslim sırasında içerik anahtarını (CK 15) bir kullanıcı anahtarı ile şifrelememekte, fakat bunun yerine bir lisans (26) ve şifrelenmemiş bir içerik anahtarını (CK 15) (ayrı ayrı veya bir arada) içeren bir dizi hak (30) yayınlamakta ve bu durumda minimum olarak, şifrelenmemiş içerik anahtarı güvenli bir kanal üzerinden mübadele edilmektedir. Alıcı cihaz (16C) lisansa bağlı olan olan kullanıcı bilgilerini (22) kontrol etmektedir. Hak yayıncısının içerik sağlayıcıdan (20) kullanıcı bilgilerini (22) içerik anahtarıyla (CK 15) veya kullanıcı hak yayıncısından (18) lisansı (26) satın aldığında doğrudan kullanıcıdan elde edebildiği bilinmelidir.

Alıcı cihaz, şifrelenmiş bir içerik anahtarı (34) üretmek için uygun gelen kullanıcı anahtarı (KA 19) içerik anahtarını (CK 15) şifrelemek için bir şifreleme sistemi (24) kullanmaktadır. Kullanıcı anahtarı (KA 19) kullanıcının alanındaki (12) cihazların (16) tümünün kullanımına açılmakta ve böylelikle her bir cihaz şifreli içerik anahtarını (34) deşifre sistemi (28) ile deşifre edebilmektedir. İçerik anahtarı (CK) deşifre edildikten sonra cihaz, şifreli içeriği deşifre edebilmekte ve içeriği (C 13) yürütebilmektedir (yani oynatabilmekte, kaydedebilmekte, görüntüleyebilmektedir).

Kullanıcı tabanlı bir içerik anahtarı şifreleme sisteminin bir üçüncü yapılandırması Şekil 4'te tasvir edilmektedir Bu yapılandırmada kullanıcı (örn. Kullanıcı A) bir lisans satın almakta, hak yayıncısı (18) içerik anahtarını (CK), hak yayıncısı (18)

tarafından atanan bir kullanıcı anahtarını (KA 19) kullanarak şifrelemektedir. Sonrasında hak yayıncısı (18) (ayrı ayrı veya bir arada) bir lisans (26) ve şifreli içerik anahtarını (34) içeren bir dizi hak (30) yayınlamaktadır. Hak yayıncısı (18) ayrıca kullanıcı anahtarını (KA 19) alandaki (12) kullanıcıya veya bir cihaza güvenli bir kanal (36) üzerinden güvenli bir biçimde iletmektedir. Sonrasında kullanıcı anahtarı (KA 19) alan (12) içindeki tüm cihazların (16) kullanımına sunulmakta ve böylece her bir cihaz şifreli içerik anahtarını (34) bir deşifre sistemi (28) ile deşifre edebilmektedir.

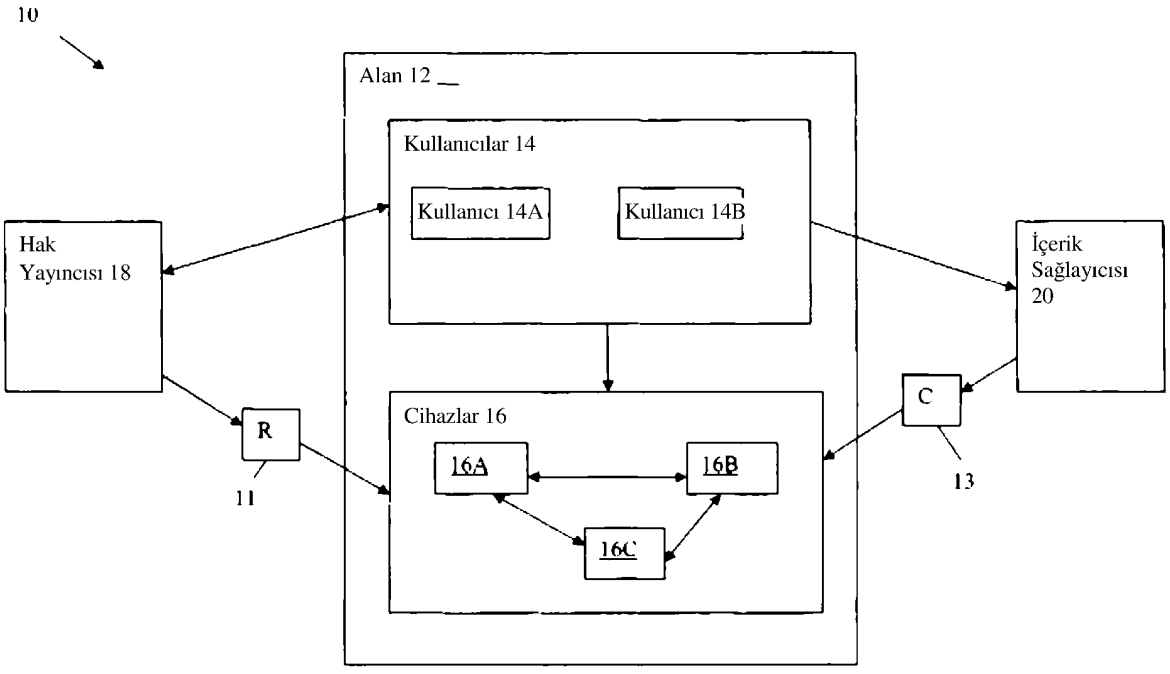
Dolayısıyla bu üçüncü yapılandırmada hak yayıncısı (18) kullanıcı anahtarlarını kullanıcılara atamaktadır. Bu yüzde bir kullanıcının farklı hak yayıncılarından üretilen çok sayıda kullanıcı anahtarı olabilmektedir. Bir kullanıcı gelecekte ilave lisanslar satın aldığında Hak Yayıncısı kullanıcıyla ilişkili kullanıcı anahtarını yeniden kullanabilmektedir.

Bu tarifnamede tarif edilen sistem, işlevler, mekanizmalar, yöntemler, motorlar ve modüllerin donanımda, yazılımda veya donanım ve yazılımın bir kombinasyonda uygulanabileceği anlaşılmaktadır. Belirtilen öğeler, herhangi bir tür bilgisayar veya bu tarifnamede tarif edilen yöntemleri gerçekleştirmek için uyarlanmış diğer aparat yoluyla uygulanabilmektedir. Tipik bir donanım ve yazılım kombinasyonu, yüklendiğinde veya çalıştırıldığında bilgisayar sistemini, bu tarifnamede tarif edile yöntemleri gerçekleştirecek şekilde kontrol eden bir bilgisayar programı bulunan genel amaçlı bir bilgisayar sistemi olabilir. Alternatif olarak buluşun işlevsel görevlerinden bir veya daha fazlasını gerçekleştirmek için uzmanlaşmış donanım içeren özel kullanımlı bir bilgisayardan yararlanılabilir. Bir başka yapılandırmada buluş kısmen veya tamamen, örneğin Internet gibi bir ağ üzerinden dağıtılmış bir şekilde uygulanabilmektedir. Bundan başka buluş, bir hizmet sağlayıcısı tarafından bir ağ üzerinden bir iş yöntemi veya hizmet olarak da sunulabilir.

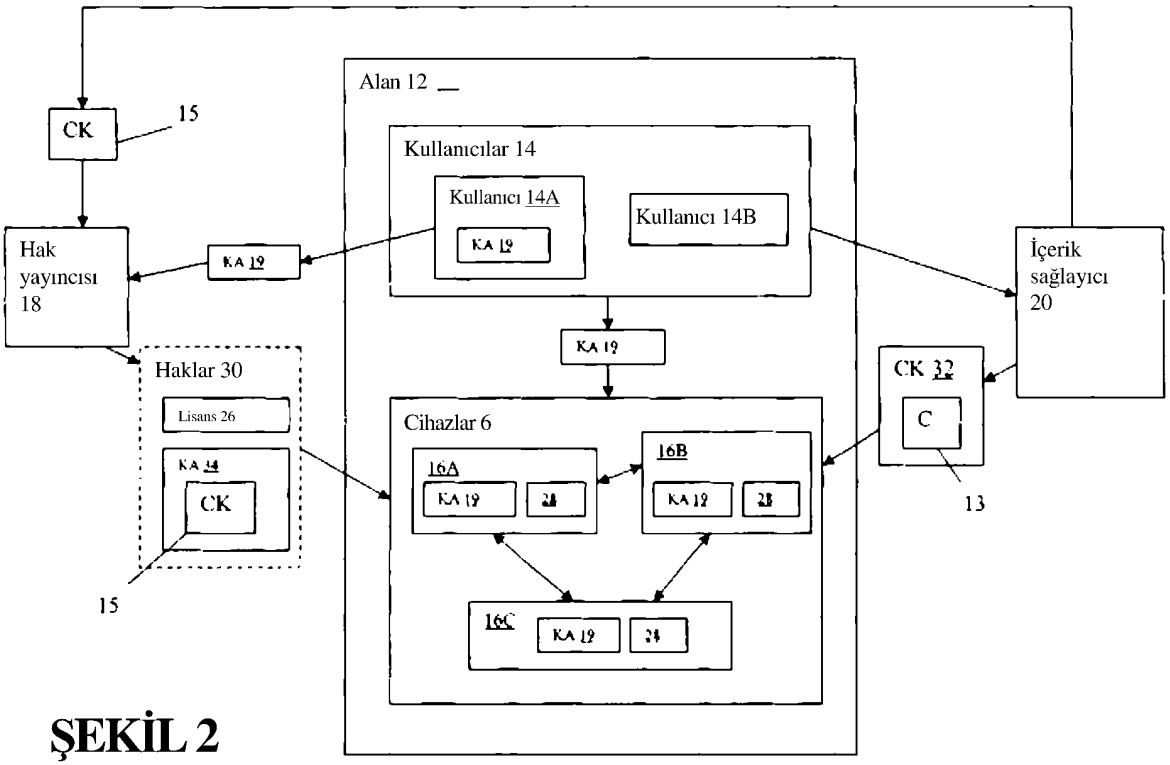
Buluş aynı zamanda, bu tarifnamede tarif edilen yöntemler ve işlevlerin uygulanmasını sağlayan tüm özellikleri içeren ve bilgisayar sistemine

yüklendiğinde bu yöntem ve işlevleri gerçekleştirebilen bir bilgisayar programı ürünü içine gömülebilir. Bu kapsamda bilgisayar programı, yazılım programı, program ürünü, yazılım vb. gibi terimler doğrudan veya aşağıdaki işlemlerin biri veya her ikisinden sonra, bilgi işleme kapasitesine sahip bir sistemin belirli bir işlevi gerçekleştirmesini sağlamak üzere oluşturulmuş, herhangi bir dilde, kodda veya gösterimdeki her türlü ifade anlamına gelmektedir: (a) bir başka dile, koda veya gösterime dönüştürme ve/veya (b) farklı bir malzeme biçiminde yeniden üretme.

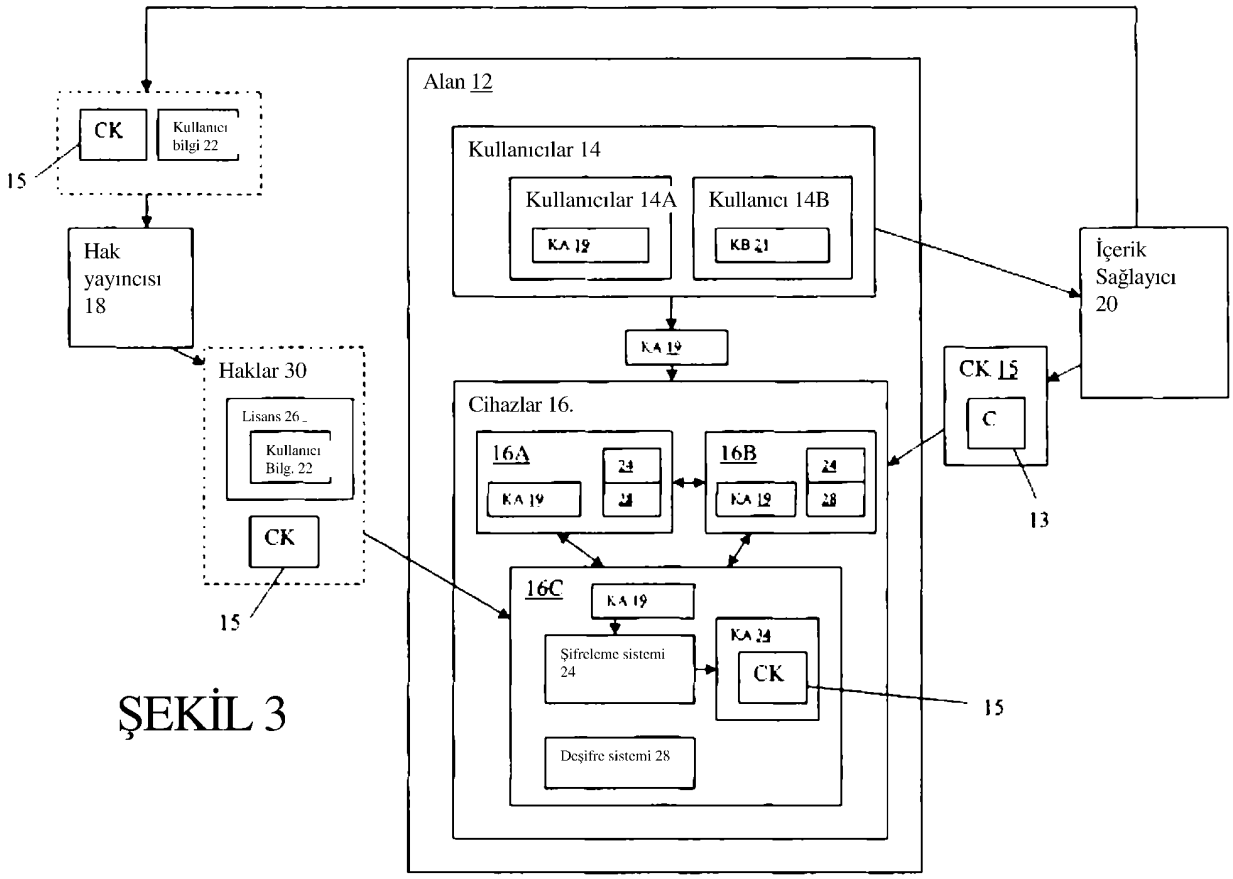
Buluşun yukarıda yer verilen tarifi örnek verme ve tarif amacıyla sunulmuştur. Teferruatlı olması veya tarif edilen kesin biçimle sınırlı olması amaçlanmamakta olup pek çok değişiklik ve çeşitlemenin mümkün olduğu açıktır. Teknikte uzman bir kişi tarafından anlaşılabilecek olan bu tür değişiklik ve çeşitlemelerin ekli istemlerle tarif edildiği gibi bu buluşun kapsamı içine dâhil olması amaçlanmaktadır.


10
Alan 12
Kullanıcılar 14
Kullanıcı 14A
Kullanıcı 14B
Hak
Yayıncısı 18
İçerik
Sağlayıcısı
20
Cihazlar 16
16A
16B
16C
R
11
C
13

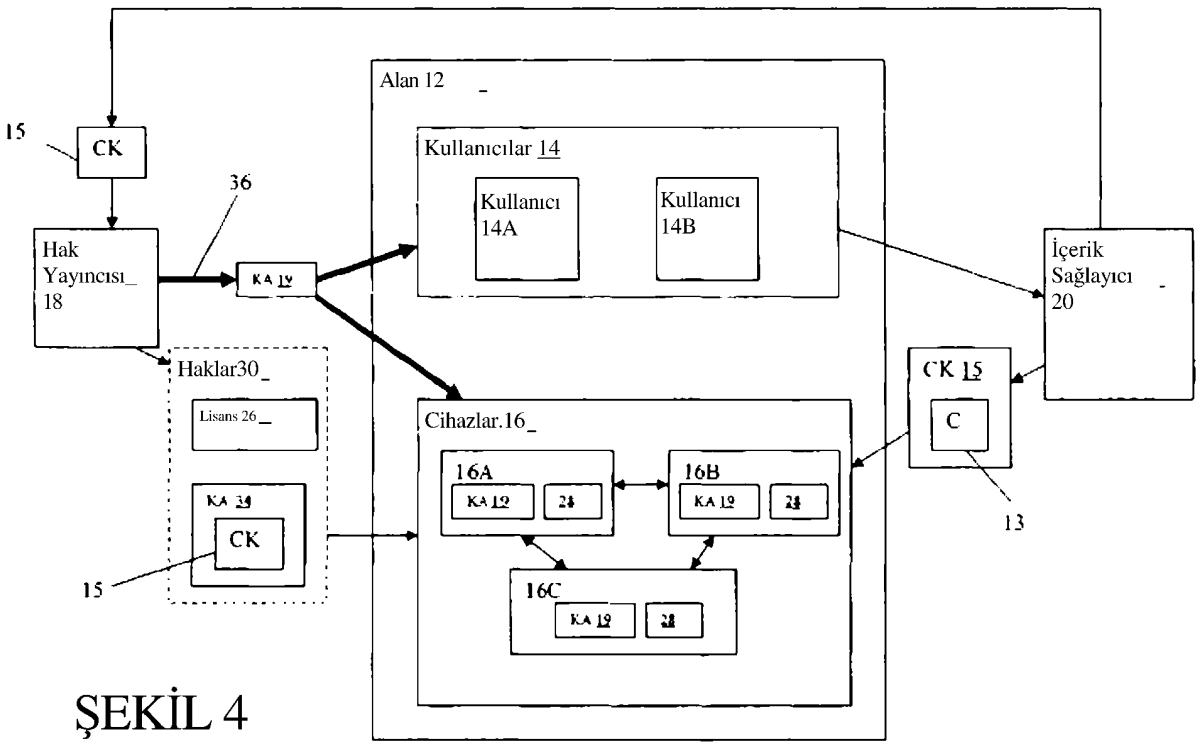
ŞEKİL 1


Alan 12
CK
15
Kullanıcılar 14
Kullanıcı 14A
KA 19
Kullanıcı 14B
Hak yayıncısı 18
KA 19
İçerik sağlayıcı 20
KA 19
Haklar 30
Lisans 26
KA 14
CK
15
Cihazlar 6
16A
KA 19
28
16B
KA 19
28
16C
KA 19
28
CK 32
C
13

ŞEKİL 2


CK
Kullanıcı bilgi 22
15
Hak yayıncısı 18
Haklar 30
Lisans 26
Kullanıcı Bilg. 22
CK
15
Alan 12
Kullanıcılar 14
Kullanıcılar 14A
KA 19
Kullanıcı 14B
KB 21
KA 19
Cihazlar 16.
16A
KA 19
24
28
16B
KA 19
24
28
16C
KA 19
Şifreleme sistemi 24
KA 24
CK
Deşifre sistemi 28
15
İçerik Sağlayıcı 20
CK 15
C
13

ŞEKİL 3


15
CK
36
Hak
Yayıncısı
18
KA 19
Alan 12
Kullanıcılar 14
Kullanıcı
14A
Kullanıcı
14B
İçerik
Sağlayıcı
20
Haklar30
Lisans 26
KA 34
CK
15
Cihazlar.16
16A
KA 19
28
16B
KA 19
28
16C
KA 19
28
CK 15
C
13

ŞEKİL 4