Proxy Architecture on DRM Service

draft-zhipeng-pkix drm-proxy-architecture-01

Zhipeng Zhou
Huawei Technologies
Background(1)

• DRM specifications have been published, such as OMA DRM2.x
  – The DRM specifications have researched the scenarios on DRM Services, such as “Join Domain”, “Acquire Rights”, etc.
  – The DRM protocols towards the DRM services have been standardized in the DRM specs.
Background(2)

• The PKI is the base stone of the DRM security.
• The trust mechanism have been well researched in the area.
• CRL service is rather mature for verifying the status of device in the service.
Scenarios for this draft

• Proxy entity in the service architecture
  – Monitor or control the entities under the proxy.
  – Simplify the service implementation for multiple personal devices.
  – Well fulfill the DRM services.
Proxy Architecture

+---------+ DRM Request +---------+ Proxy DRM Request +---------+
| Request | ------------> | Proxy     | --------------> | Service |
| Device A | <------------  | Device B  | <-------------- | Server |
+---------+ DRM Response +---------+ Proxy DRM Response +---------+
Trust Architecture for proxy DRM Service

Certificate A

+-----------------+ Authorization +-----------------+ Authorization +-----------------+
|- Request | ---------------| Proxy | ---------------| Service |
| Device A | ---------------| Device B | ---------------| Server |
+-----------------+ DRAM Response +-----------------+ Proxy DRM Response +-----------------+
Authorization Document

- The key media used to construct the trust chain for the DRM proxy service
- The Authorization Document is composed of:
  - -- name of Request Device
  - -- CertId of Request Device
  - -- name of Proxy Device
  - -- CertId of Proxy Device
  - -- authorized service rights
  - -- extensions
  - -- signature algorithm
  - -- signature
Multiple-Proxy Architecture
Trust Architecture for Multiple-Proxy DRM Service

```
            +                   +                   +
            +------------------ Authorization ------------------+
|Request | ---------------------|Proxy | ---------------------|Proxy | ---------------------|
            | Device A |------------------|Device-1 |------------------|Device-n |
            +------------------ DRM Response |------------------|
            +------------------ Certificate-A |
            +------------------ Proxy |
            +------------------ DRM Response-1 |
            +------------------ Certificate-A |
            +------------------ Proxy |
            +------------------ DRM Response-n |
```

Service  
| Server  
|--------- Proxy DRM Response-n  


Standardization

• The architecture of proxy DRM service;
• The trust architecture for proxy DRM service;
• The Authorization Document.
Questions

- Comments welcome.
- Thanks.