Trust Services for OMA Digital Rights Management

The Information Security Problem

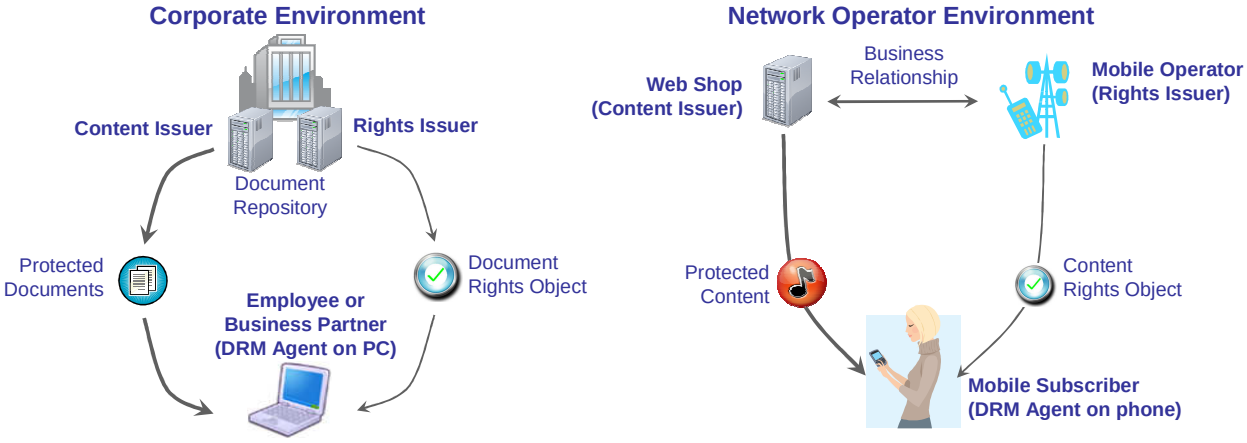
Increasingly organisations need to enhance the security of their information assets. Controlled access to this core information needs to be granted to employees, contractors, partners, auditors and a variety of external entities. The data should only be visible to those with a defined 'need to know' and if their role changes then the rights should be removed.

Mobile Information Security

Content providers and Mobile Network Operators have strong business drivers to make downloadable content available to their fee paying subscribers. They wish to ensure that this valuable content cannot be freely distributed, however it is a clear benefit to have the content passed on to others to stimulate demand for paid access rights.

The OMA DRM 2.n Solution

The following diagrams illustrate typical scenarios where the Open Mobile Alliance (OMA) Digital Rights Management (DRM) specifications are used to provide content protection services. Access to the content is restricted by using local "DRM Agent" software that applies the appropriate "Rights Objects" supplied by the Rights Issuers.



In the OMA DRM 2.n model there are four actors: DRM Agents; Content Issuers; Rights Issuers; and Trust Service Providers.

- DRM Agents: This is security software that is appropriate for mobile phone or desktop use. It enables individuals to download and access encrypted content. Depending on the context the users are individual mobile phone subscribers or company employees. The DRM Agent restricts access to the content as defined within the Rights Object.
- Content Issuers: These entities are responsible for protecting and delivering the documents, music or video files to the DRM Agents. Examples of Content Issuers are Web Shops and Corporate Document Repositories.
- Rights Issuers: These entities are responsible for creating the Rights Objects that cryptographically control access to the data content. Typically they are Mobile Network Operators, Companies and potentially other organisations.
- Trust Service Providers: These entities operate the Certification and Validation Authorities that that permit the OMA DRM 2.n model to function securely.

OMA DRM Trust Service Requirements

CAs are required for issuing digital certificates to DRM Agents and Rights Issuers. OCSP Validation Authorities are required to provide real-time certificate status information to enable:

- Rights Issuers to authenticate the DRM Agents
- DRM Agents to authenticate the Rights Issuers

Rights Issuers are then able to create Rights Objects for specific content and specific DRM Agents by encrypting the content keys and the access rights under the DRM Agent certificates.

Ascertia Trust Service Products

Ascertia supplies two products that are relevant for providing OMA DRM 2.n Trust Services:

- TrustFinderOCSP - this provides the OCSP Responder (Validation Authority) services for the Rights Issuer CA and/or the DRM Agent CA.
- TrustFinderCA – this provides Certification Authority services for issuing certificates to the Rights Issuers and DRM Agents.

TrustFinderOCSP

TrustFinderOCSP is an RFC2560 compliant OCSP Responder certificate validation. TrustFinderOCSP has been designed to operate as a robust validation hub solution, capable of providing OCSP certificate validation services for multiple Certificate Authorities (CAs). It offers class-leading flexibility for request and response handling, throughput and availability. It provides simple to use yet sophisticated management controls and reporting. It is well-proven in production use with the OMA DRM, Financial, Government and Telco markets.

TrustFinderCA

TrustFinderCA is an RFC3280 compliant Web Services CA for certificate issuance and management. Certificate Authority services are offered via high level XML/SOAP web services. These certification services can be easily integrated within a business application or a dedicated Registration Authority. In such cases Ascertia can also deliver business focused Registration Authority solutions to meet specific project requirements.

Test Services – www.GlobalTrustFinder.com

One of the problems for organisations that are developing DRM Agent and Rights Issuer software and solutions is the ability to access suitable test systems. Ascertia has spent a substantial amount of time building a technology interoperability test site called GlobalTrustFinder.com (or GTF for short). The purpose of the site is to demonstrate the ease with which trust technologies and services can be used – and in some cases within example business scenarios. For OMA interop test purposes Ascertia is willing to offer free access to its TrustFinderOCSP powered GTF validation services. As part of the usage agreement the relevant issuer CAs for the Rights Issuer and DRM Agent will be configured.

Shortly GlobalTrustFinder.com will be extended to deliver test certificates for DRM Agents and Rights Issuers. These services are intended to assist with industry interoperability testing, product testing as well as project feasibility testing. Of course the TrustFinderOCSP and TrustFinderCA products can also be licensed for delivery within test or production systems.

For further information on these products; or the GlobalTrustFinder test website; contact us via e-mail at sales@ascertia.com or visit our website at www.ascertia.com.