



Security for Virtual Collaboration

Access Control & DRM

Presented by: **Adrian Waller**

VISNET II Industry Day

TI Lab, Turin, 20th May 2008

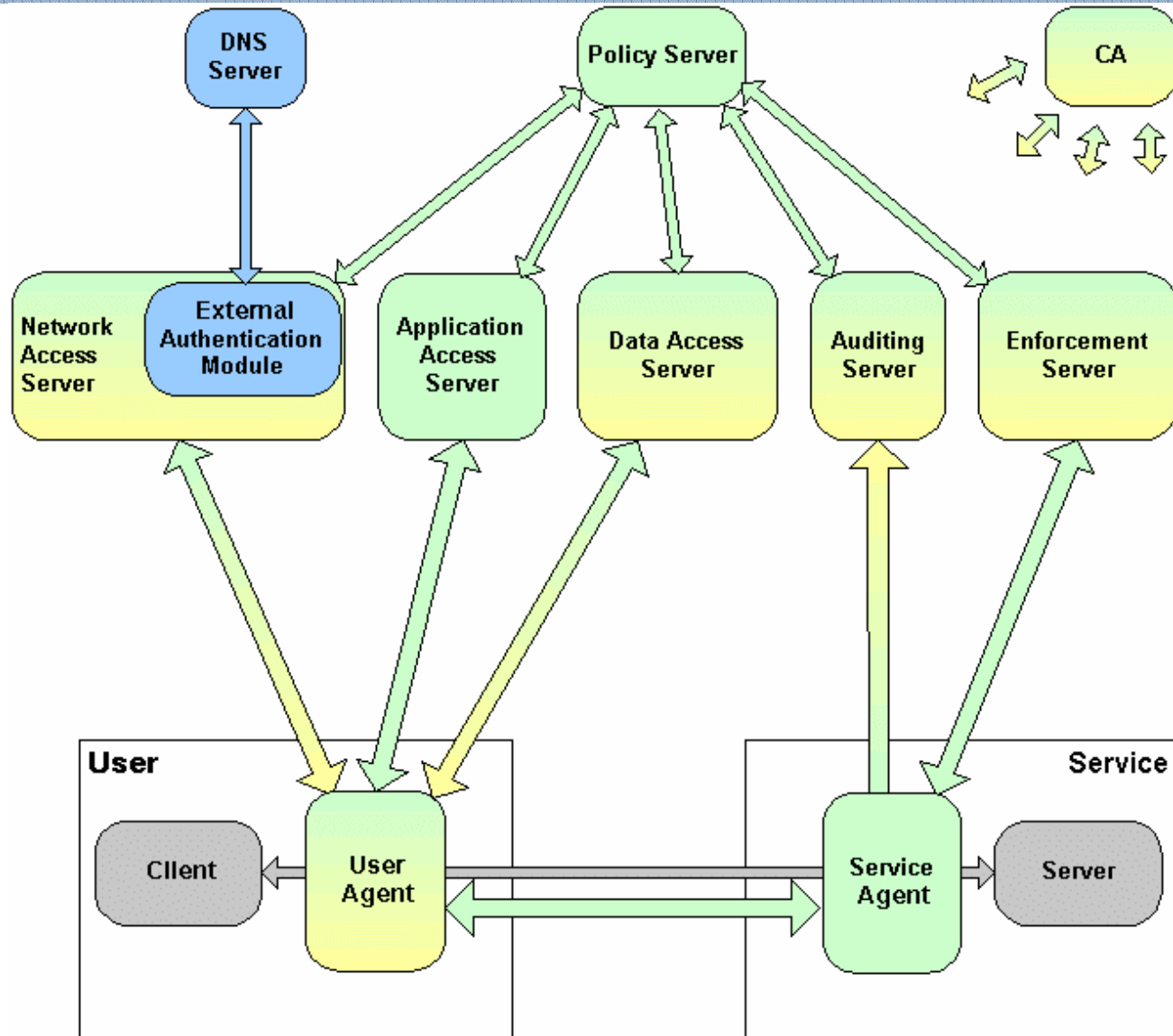
- **Requirements for virtual collaboration**
- **Access Control Architecture**
- **DRM Architecture**
- **Bringing it all together**
 - An integrated solution

- **Multiple users from multiple organisations connecting together to work collaboratively**
 - May not have full trust in each other
 - May have their own policies and goals and wish to keep control of their resources (Networks, Systems, Applications, Data and Users)
 - May have different security implementations
- **Such collaboration could be short-term or long term, static or dynamic**
 - Virtual meeting (short-term, fairly static)
 - Crisis management (medium-term, highly dynamic)
 - Joint project (long-term, moderately dynamic)
- **Ad-hoc and dynamic integration of resources across organisational boundaries to support collaborative working is needed**
 - Resources need protecting in this potentially volatile environment
 - Highly sensitive data, such as commercial, personal or even governmental data, may need protecting

Access control issues

- **Resources owned by multiple organisations with multiple policies**
- **Policies may need to be set up on demand, and may change over time at short notice**
- **No common security control point, security architecture or security mechanisms exist across the Virtual Collaboration**
 - One technical solution cannot be enforced
- **Currently, access control is typically managed separately for individual systems**
 - Impractical, both from an administrator's and end user's point of view (e.g. having to remember many passwords).
- **Need a simplified and consistent approach**
 - VISNET II developing a Federated Identity Management architecture
 - Based on WS-Federation, but tailored to virtual collaboration and high security scenarios

Access control architecture



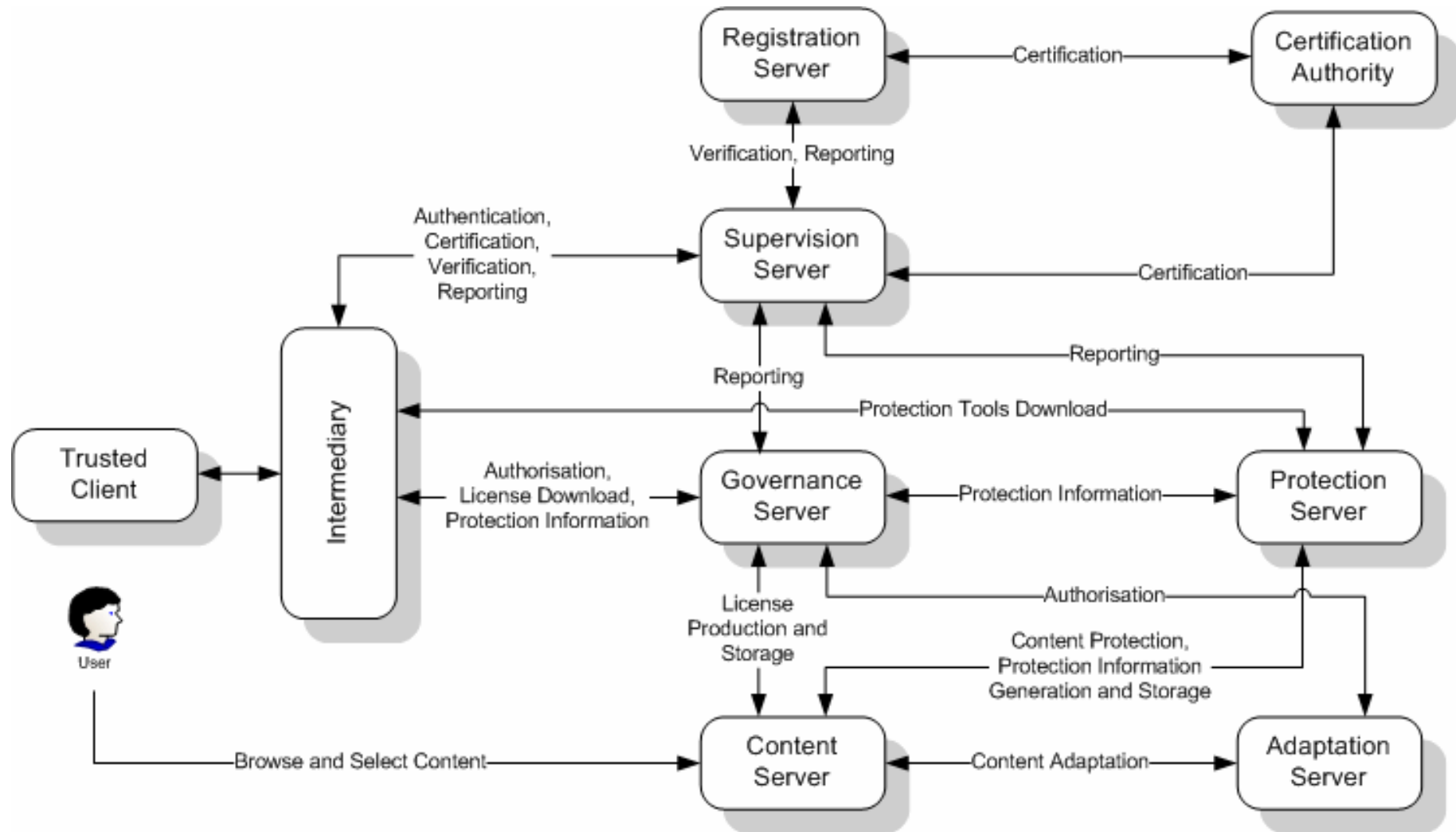
- **User and Service Agents**
 - Intercept requests from users to access services to obtain and provide authorisation tokens to Service Agents
- **Network Access Server**
 - Authenticates users and returns authorisation tokens
 - Translates tokens & roles between networks
- **Application/Data Access Server**
 - Authorises access to resources based on supplied (network) token
 - Returns a (resource) authorisation token
- **Auditing Server**
 - Keeps a record of access to services by users for auditing purposes, and to allow rapid revocation (see below)
- **Enforcement Server**
 - Uses information from the Auditing Server to immediately revoke access to services that a user is no longer permitted to access

■ Many DRM initiatives

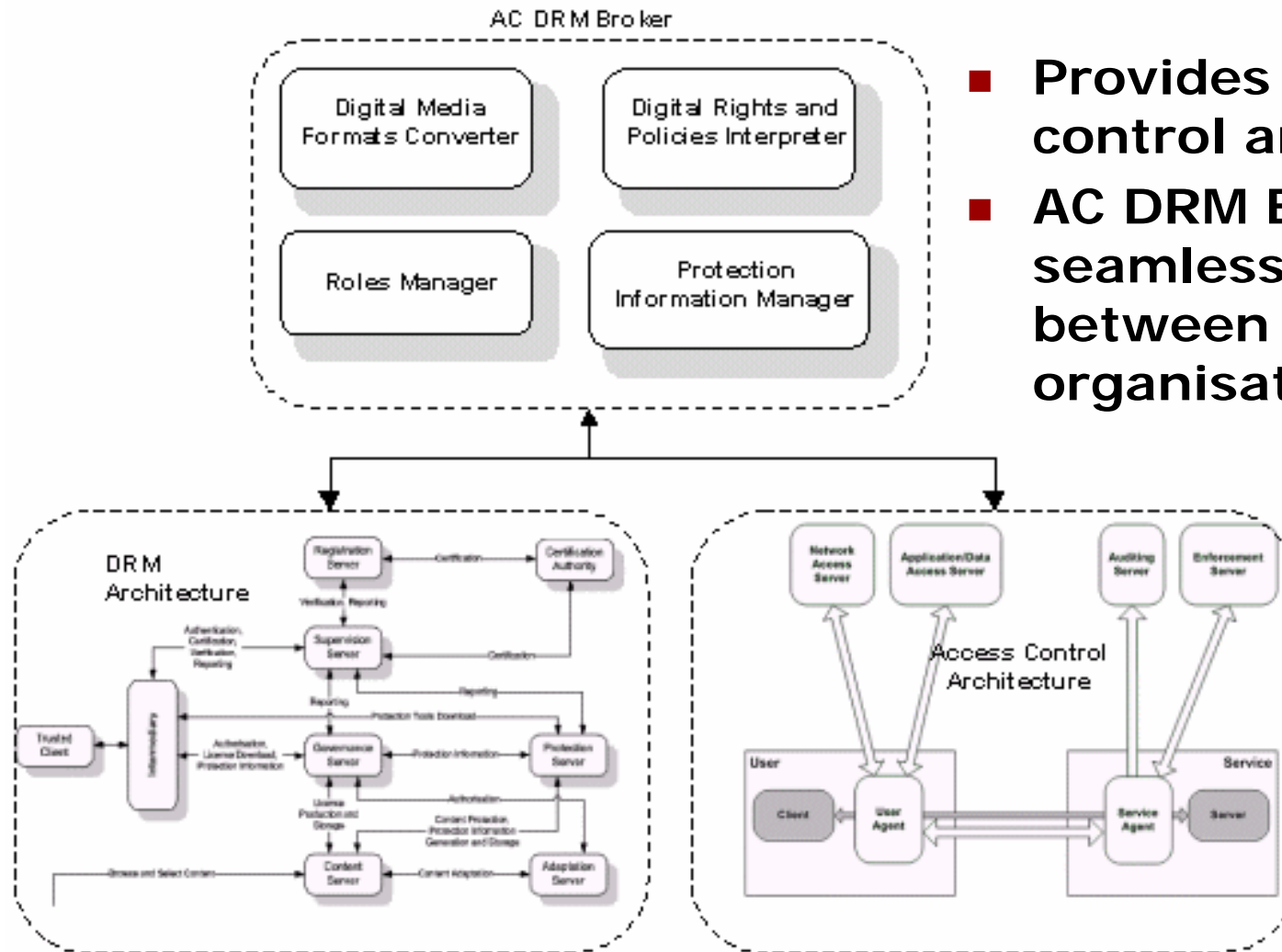
- E.g. MPEG-21, Open Mobile Alliance (OMA), Windows Media and Apple Fairplay
- Multiple fragmented solutions leads to interoperability problems in Virtual Collaboration
- Aimed at high-value multimedia content purchasing (I.e. not Virtual Collaboration)

■ VISNET II developing

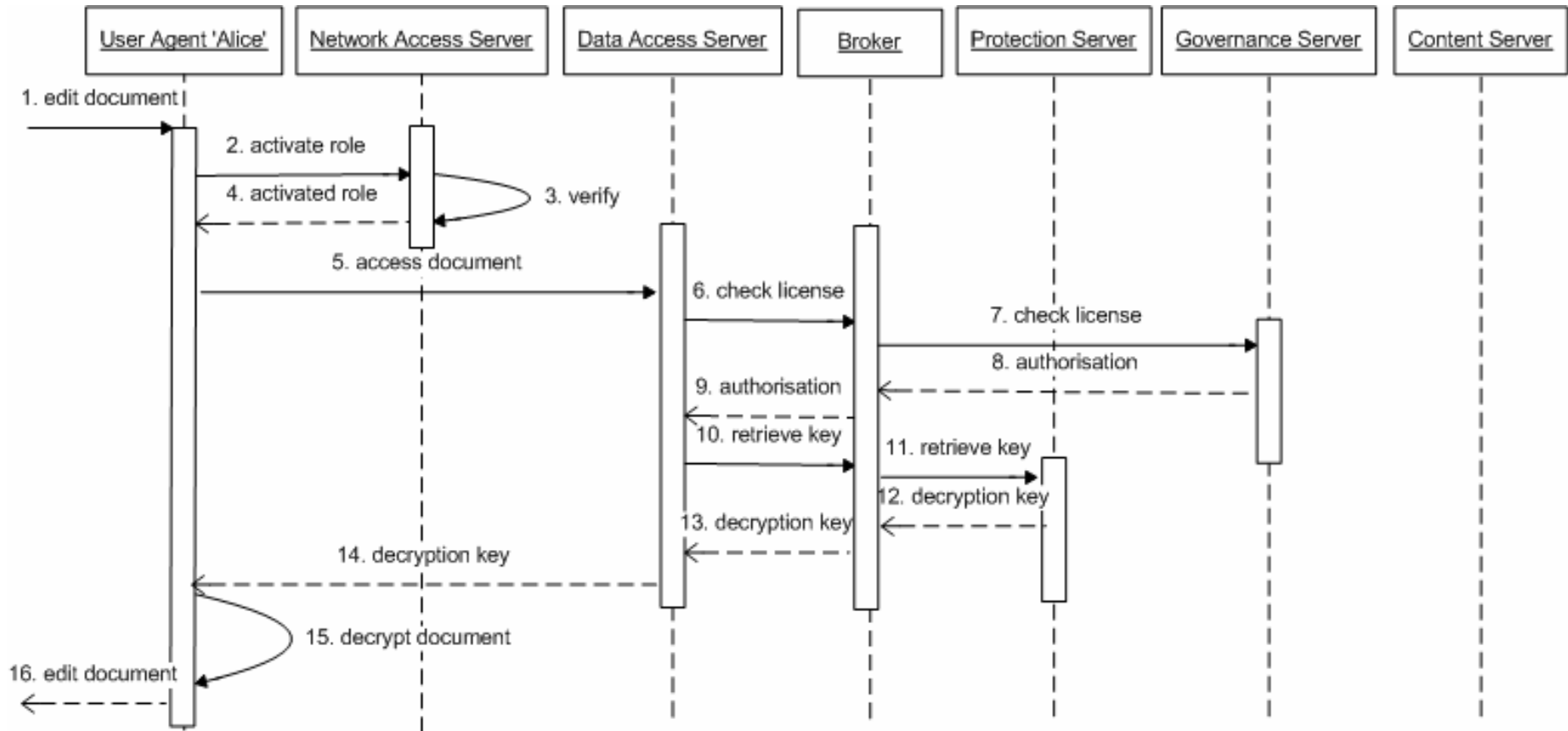
- Standards based (Web Services) interoperability architecture for DRM
- Interoperability 'Broker' to manage multiple DRM implementations
- Integration of this architecture with virtual collaboration



- **Content Server**
 - Enables users to browse/select/download content
 - Adds metadata to raw content and stores the created digital objects.
- **Supervision Server**
 - Authenticates and supervises actors and system components
 - Manages event reports about content consumption
- **Governance Server**
 - Creates and stores licenses
 - Performs online license-based authorisation
 - Translates licenses between different rights expression languages.
- **Protection Server**
 - Protects digital objects and generates, stores and delivers protection keys and protection information
- **Trusted Client**
 - Creates and edits digital objects, and manages event reports and metadata



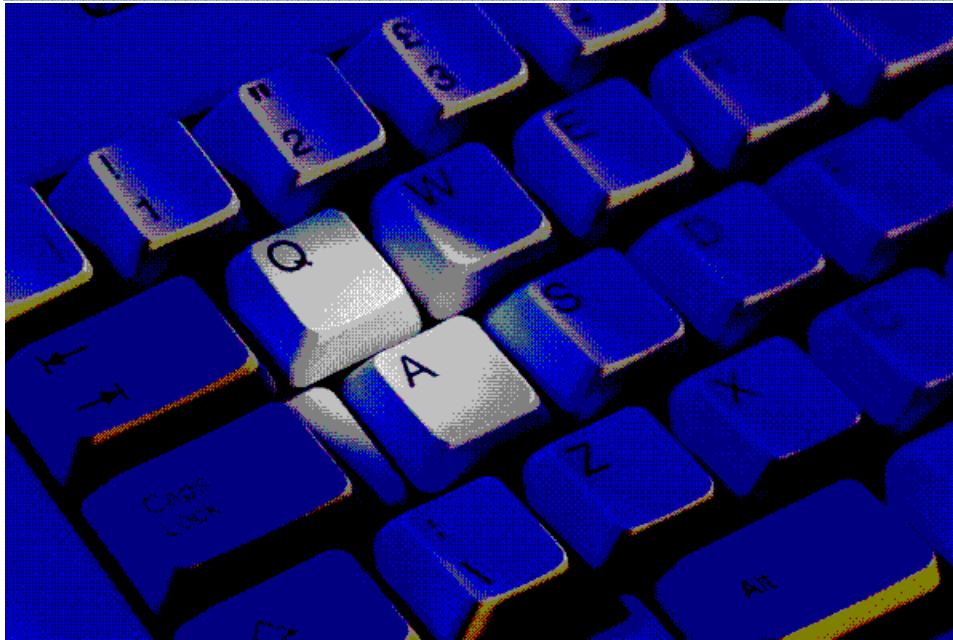
- Provides integrated access control and data management
- AC DRM Broker provides seamless interoperability between multiple organisations



A user 'Alice' retrieves a protected document for editing

- **Protecting resources in Virtual Collaborations can be a highly complex task**
- **VISNET II is developing novel security solutions that:**
 - Make management of users and their access rights flexible, simple and interoperable with existing implementations
 - Leverage sophisticated data security management capabilities of existing DRM systems
 - Enables fine-grained and flexible access control on data
 - Without the interoperability drawbacks that currently hamper their use
 - Integrated with overall management of access control to resources
 - Are capable of supporting a wide variety of scenarios
 - From static to highly dynamic
 - From short-term to long-term
 - From low security to highly sensitive scenarios

Thank You!..



THALES



Contact:



Jaime.Delgado@ac.upc.edu (UPC&UPF)

Adrian.Waller@thalesgroup.com (Thales)

Maria.Andrade@inescporto.pt (INESC)