



## Who we are

**University of Siegen** (North Rhine Westfalia, Germany)  
**Department of Electrical Engineering and Computer Science**

**Institute for Data Communications Systems**

**Director: Prof. Dr. Christoph Ruland**

**Project Leader Digital Broadcasting: Dipl.-Wirt-Inform. Sibylle Müller**

**Address:** Hoelderlinstrasse 3, D-57076 Siegen / Germany  
**e-mail:** {christoph.ruland, sibylle.mueller}@uni-siegen.de  
**url:** www.dcs.uni-siegen.de

- **Research Area:**
  - ❖ Integration of Security into Communications Systems
- **Staff of the Institute:**
  - ❖ 15 employees (10 scientific assistants, 5 non-scientific members)
  - ❖ in 2005: 6 Dr.-Ing. Graduations
- **Experiences (last 5 years):**
  - ❖ 8 EU-Projects (4th, 5th, 6th Framework, CRAFTS, ISIS)
  - ❖ Project leader, workpackage leader
  - ❖ 5 Projects by national research programs
  - ❖ 8 Industrial projects
- **Standardization:**
  - ❖ Active Member in ISO SC 27 (formerly SC 20) "Security Techniques" (3 Project Editors)



## Previous Work on Digital Broadcasting

- **Project:**  
**"Security System for Multimedia Multicast Communication over the Internet"**  
 Project funded by DFG (National German Research Organization) in 2002 – 2005
- **Solution:**  
**Differentiated Authentication Services for Real-time Multimedia Streaming over the Internet**
- **Differentiated Digital Signatures:**
  - ❖ EP (Expedited Processing) Signature for short term data origin Authentication
  - ❖ AP (Assured Processing) Signature for support of (long term) Non Repudiation of Origin and key distribution for EP Signatures
  - ❖ Calculation of key lengths depending on the period of validity of security
  - ❖ Multiplexed Digital Signatures for multi-sessions
    - ❖ Multimedia (Audio/Video/Animation)
    - ❖ Multi-rate video multicasting
- **Differentiated Signatures protocol specification for SRTP**  
 (Secure Real Time Transport Protocol)





## Proposal for our part in a Digital Broadcasting project with China & Latin America

### Security in Digital Broadcasting:

- Short term Authentication on the fly (during transmission and reception)
- Long term Non Repudiation of Origin Security Service
- Cooperation with digital watermarking systems/ video-/audio-codec-developers
- Support of security for hierarchical compression Codecs
- Focus on:
  - ❖ Synchronization
  - ❖ Error Propagation
  - ❖ Robustness
  - ❖ Performance
  - ❖ Implementation on Special Hardware (e.g. Signal Processors, FPGA)

### Our tasks

- Participation in:
  - ❖ Business Model, Scenarios
  - ❖ Design of the System and Security Architecture
  - ❖ Definition of Security Mechanisms and Protocols
  - ❖ Specifications
  - ❖ Implementation
  - ❖ Integration
  - ❖ Field Test
- Provision of Key Management/Security Infrastructure