**Segurança de Redes e Sistemas de Computadores**

**2018/2019, 2º Sem.**

**Ficha de Implementação do Trabalho Prático nº 1**

***Secure Real Time Media Streaming System***

**Grupo**

**Nº NNNNN Nome Apelido**

**Nº NNNNN Nome Apelido**

Notas: YOu can write this report in English or Portuguese. You can also use WORD or LaTeX (using in this case a format from IEEE, ACM or Springer in the end of this document). As you can find, sections 1, 2 and 3 can be iterated (more or less directly) from the initial specifications for TP1, according to your specific implementation. Sections 4 and 5 are only for the solution and implementation of Phase 2. Section 5 is a section for Conclusions, Open Issues, as well as, Lessons and Remarks from your experience in implementing the TP1.

***Abstract***

1. **Introduction**
2. **System Model and Architecture**
   1. **System Model and Components**
   2. **System Architecture**
   3. **Adversary model definition**
3. **Secure Channel and Runtime Support with Static Configuration (Phase 1)**
   1. **Protocol Specification**
   2. **Runtime support**
   3. **System configuration**
4. **Stream-DTLS protocol with dynamic configurations (Phase 2)**
   1. **System model, architecture and components**
   2. **Protocol for Proxy Authentication, Payment and Ticketing (Proxy-Ticket Line Service)**
   3. **Format, Security and Validation of Payments using MovieCoins**
   4. **Tickets for Real Time Streams**
   5. **Establishment of Cryptographic Security Associations for Secure Streaming (Proxy-Stream Server)**
5. **Conclusions**
   1. **Main conclusions**
   2. **Open issues**
   3. **Lessons and Remarks**

Suggestions LaTeX Formats (you also have WORD-Reference Formats):

[**https://www.ieee.org/conferences/publishing/templates.html**](https://www.ieee.org/conferences/publishing/templates.html)

[**https://www.acm.org/publications/authors/submissions**](https://www.acm.org/publications/authors/submissions)

[**https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines**](https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines)