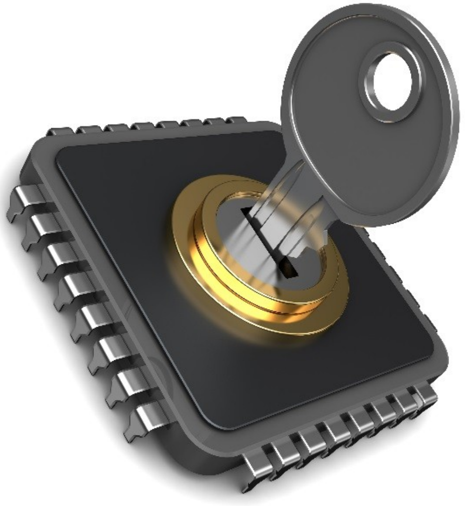
Introduction to Information Security

Kick-off Tutorial
Electronic Signatures



Winter 2015/2016

Stefan Steinegger

Organisational - Tutorials

- No further Tutorials
- Support from:
  - Newsgroup (Problems affecting more people)
    - tu-graz.lv.einfuehrunginformationssicherheit
  - Me (small problems, interesting for the group)
    - E-Mail: stefan.steinegger@student.tugraz.at
  - Meeting (bigger problem, interesting for the group)
    - Contact me for an arrangement

Timeline

- November 17th
  - Signed rule confirmation email (see Wiki)
  - Project specification
- ~ November 23th
  - Discussion of project specification
- < December 24th – inform me about progress (email)
- January 21st - Final deliverable
- ~ January 28th – Final interview

Electronic Signatures - Motivation

Why?

- Certificates are one of the most used technologies in the context of cryptography nowadays
- Needed for proof of authenticity and integrity of persons or objects

How?

- Understand how the online certificate status protocol work
- Get an insight of X.509 and certificate chains

Assignment

Proof of concept application

- Implement online certificate status protocol (OCSP) based on certificate revocation list (CLR)
- Implement a server and a client
- Able to check and verify certificates (via OCSP and general validity)
- Able to work with certificate chains
- Using the IAIK JCE library (see link in appendix)

1st Deliverable - Specification

- 2-4 pages (PDF)
- Upload via STicS
- One specification per group
- Detailed plans for implementation of server, client and protocol
- Supported features

- Will be discussed in the first meeting

2nd Deliverable – Final

- Project Documentation (PDF)
- Readme (folder structure, set up steps, software versions used,...)
- Source Code
- Test Cases
- Upload via SticS (max. size 20MB)

Next Steps

- Get IAIK JCE to work
  - Contains a lot of small example programs
- Read the RFC and IAIK JCE documentation (→ Appendix)
- Write the confirmation mail
- Make server and client talk over sockets
- Write the specification.
- Test cases
  - create CAs, intermediate CAs, Certificates,...
  - Test valid and invalid certificates!

Course wiki
https://teaching.iaik.tugraz.at/eis/start

OCSP RFC6960
https://tools.ietf.org/html/rfc6960

Java IAIK JCE (register for free educational licence):
http://jcewww.iaik.tu-graz.ac.at/sic/Sales/Licences/Educational
https://jce.iaik.tugraz.at/crm/registration.php

Java IAIK JCE documentation
http://javadoc.iaik.tugraz.at/iaik_jce/current/