Dominik Schadow

Experience XML Security

The Eclipse XML-Security Plug-In

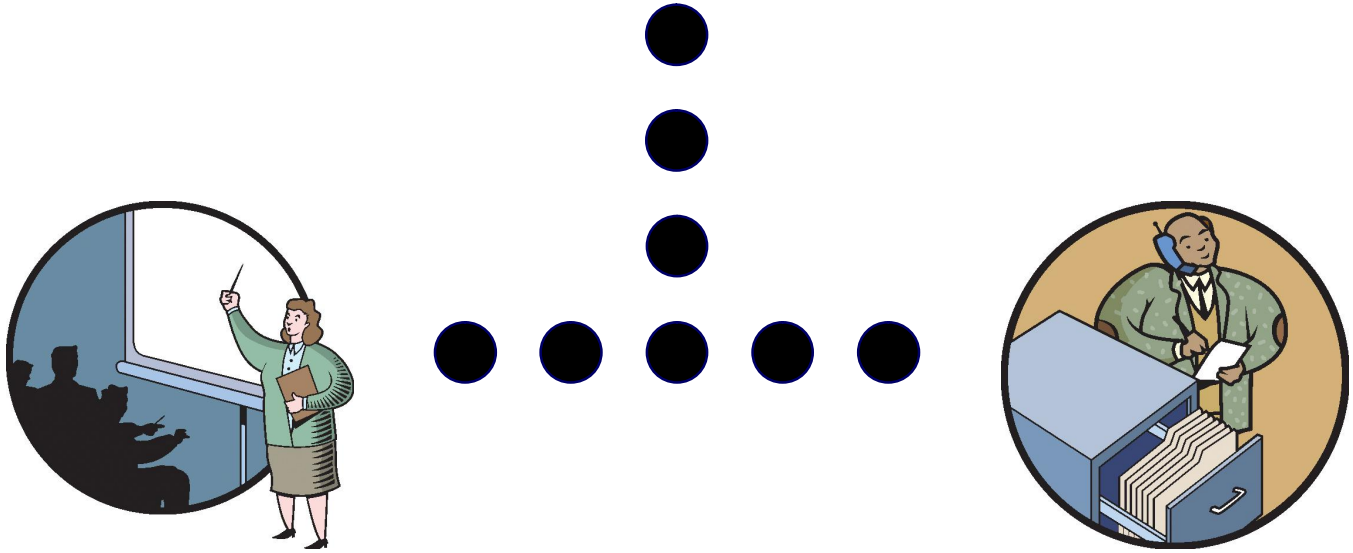
9th Conference on Communications and Multimedia Security
19 - 21 September 2005

The Future...

- everybody signs/ encrypts messages
- messages can be assigned to the sender
- private information remains private
- …

What Do We Need?

User Awareness



eLearning software education

easy to use applications

- XML Security
- XML-Security Plug-In
- CrypTool
- Comparison Plug-In ⇔ CrypTool
- JCrypTool

XML Security – Overview

- **XML Signature**
  - W3C Recommendation 12 February 2002
- **XML Encryption**
  - W3C Recommendation 10 December 2002

- information based security
- secure
  - any digital content
  - XML document fragments

XML Security – Digital Signatures

- integrity, message + signer authentication
- signature types
  - enveloping signature
    signature is parent
  - enveloped signature
    signature is child
  - detached signature
    signature is external or sibling

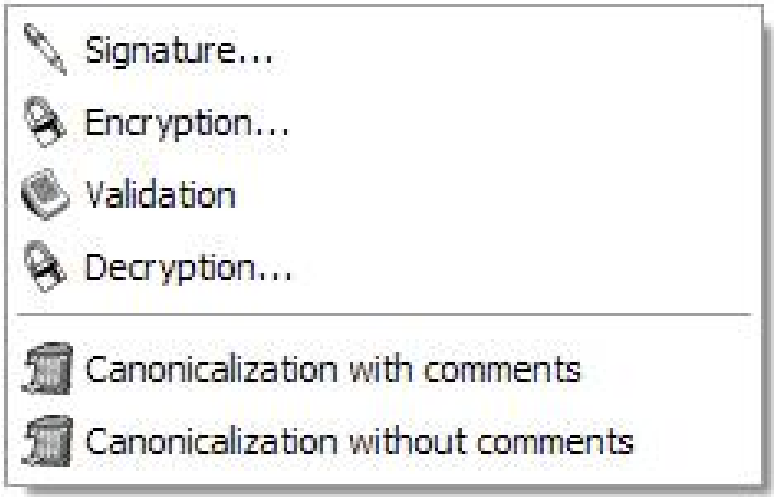
XML Security – Encryption

- confidentiality
- encryption types
  - element content
    no tags
  - elements
    including start /end tags
  - super-encryption
    multiple encryption of elements
- document structure may change

XML-Security Plug-In – Overview

- diploma thesis 2004
- XML security from scratch

- easy to use
- focus on practical application
- extensive online help



- Eclipse 3.0/3.1
- different views and most editors
- freeware

XML-Security Plug-In – Signature

Digital Signature

- step by step wizard
- combinations

Validation

- popup window
- fast usage

XML-Security Plug-In – Encryption

Encryption

- step by step wizard
- different algorithms

Decryption

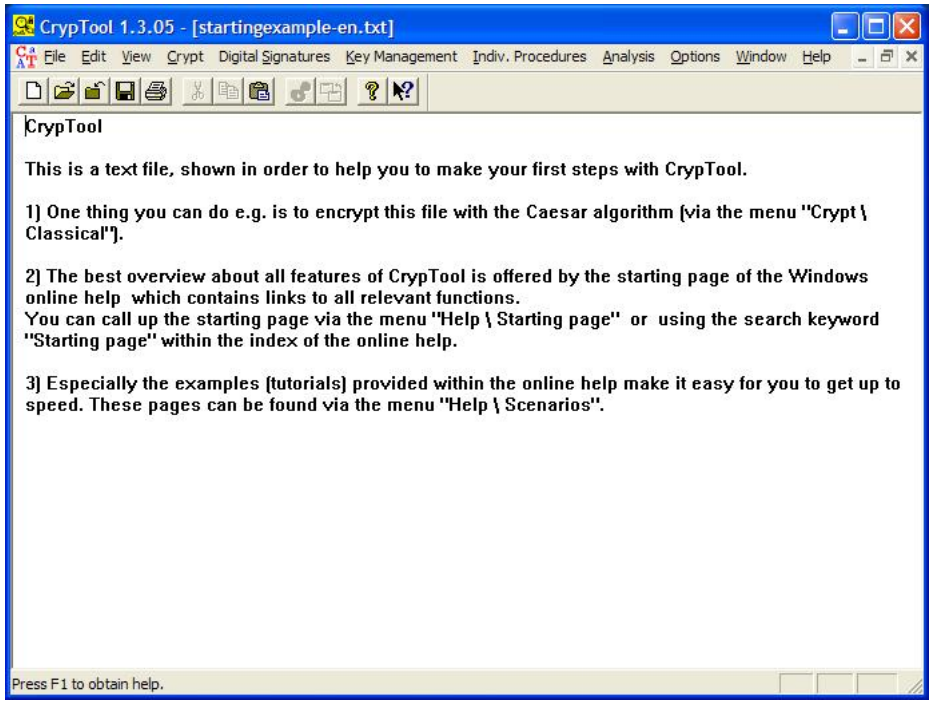
- small wizard
- select key file

XML-Security Plug-In – Help

Online Help

❶ XML Security ❷ Plug-In

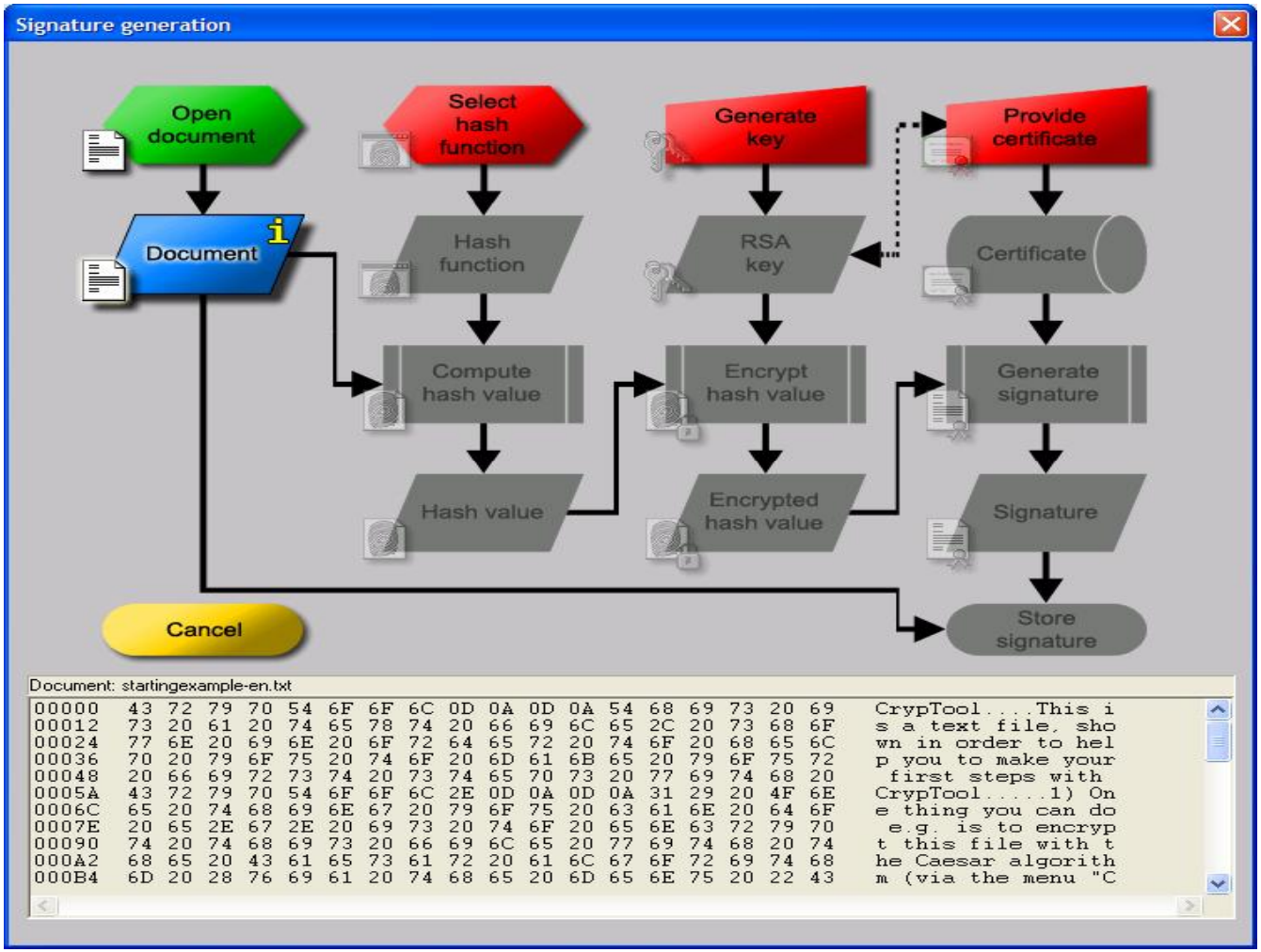
CrypTool – Overview



- creating awareness of IT security issues
- learning about and obtaining experience of cryptography
- encryption algorithms and analysis procedures
- most state of the art algorithms
- Deutsche Bank and university cooperations

CrypTool – Signature

visual signature generation…



Comparison Plug-In ⇔ CrypTool

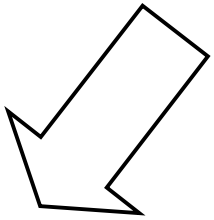
CrypTool

stand-alone application for Windows

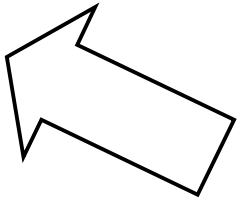
cryptography from scratch

for beginners and advanced users

extensive help for all cryptographic aspects



IT security awareness



Plug-In

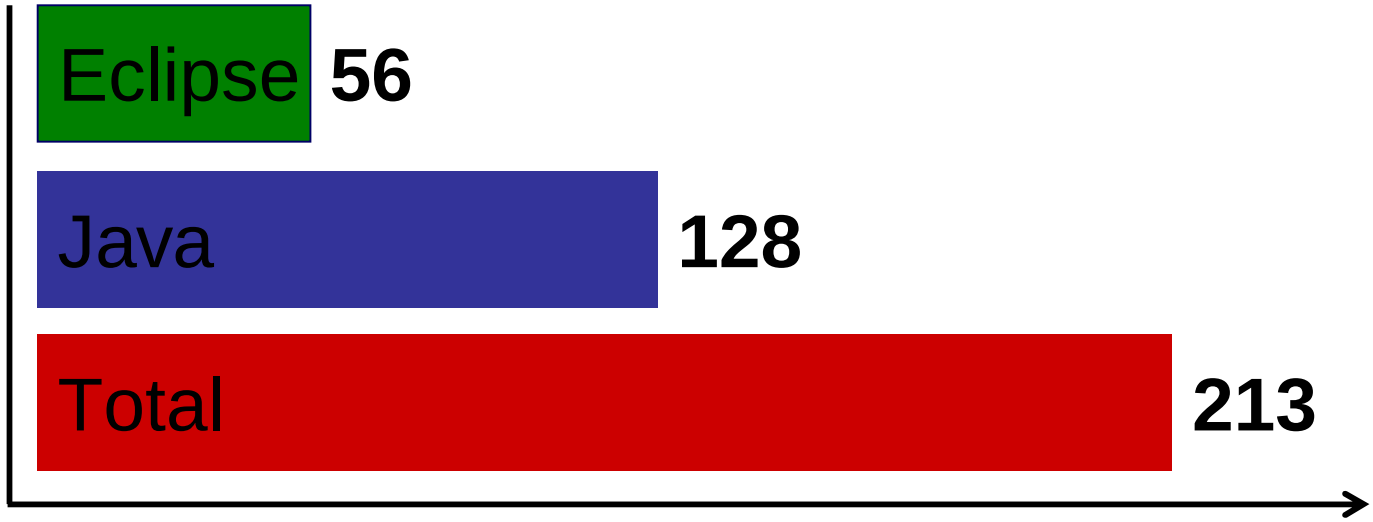
Eclipse plug-in

XML security from scratch

requires cryptographic knowledge

extensive help for XML security

JCrypTool – Overview



Eclipse Rich Client Platform

- platform independent
- extendable with plug-ins
- modern
- focus on features

JCrypTool – Features

features

- beginners and advanced users
- same functionality as CrypTool
- XML security

situation

- 5 developers
- support from Deutsche Bank
- design/ prototype development

Links/ Contact

Download
the XML-Security Plug-In and CrypTool

www.xml-sicherheit.de www.cryptool.com

Dominik Schadow
Pasingerstrasse 28
82152 Planegg
Germany

info@xml-sicherheit.de
www.xml-sicherheit.de