JCrypTool
The cryptography e-learning platform

Dominik Schadow
Consultant
Application Development
dominik.schadow@trivadis.com

Hagenberg, 20. May 2008

trivadis
makes IT easier.

Agenda

- Overview
  - Core Project
  - Plug-ins Project
- Demo
- Summary

Agenda

- Overview
  - Core Project
  - Plug-ins Project
- Demo
- Summary

Overview (1)

- **the cryptography e-learning platform**
  - encryption/ decryption
  - digital signatures
  - hash functions
  - cryptanalysis
  - XML Security
  - …
- launched January 2007
- CrypTool successor
  - learning,
  - teaching,
  - **developing** cryptography
- free, **open source**, GPL license (switch to EPL planed)

Overview (2)

- **Eclipse RCP** based (version 3.3)
  - platform independent (Java 1.5)
  - modern software design (pure plug-in architecture)

- **multi language** – German and English

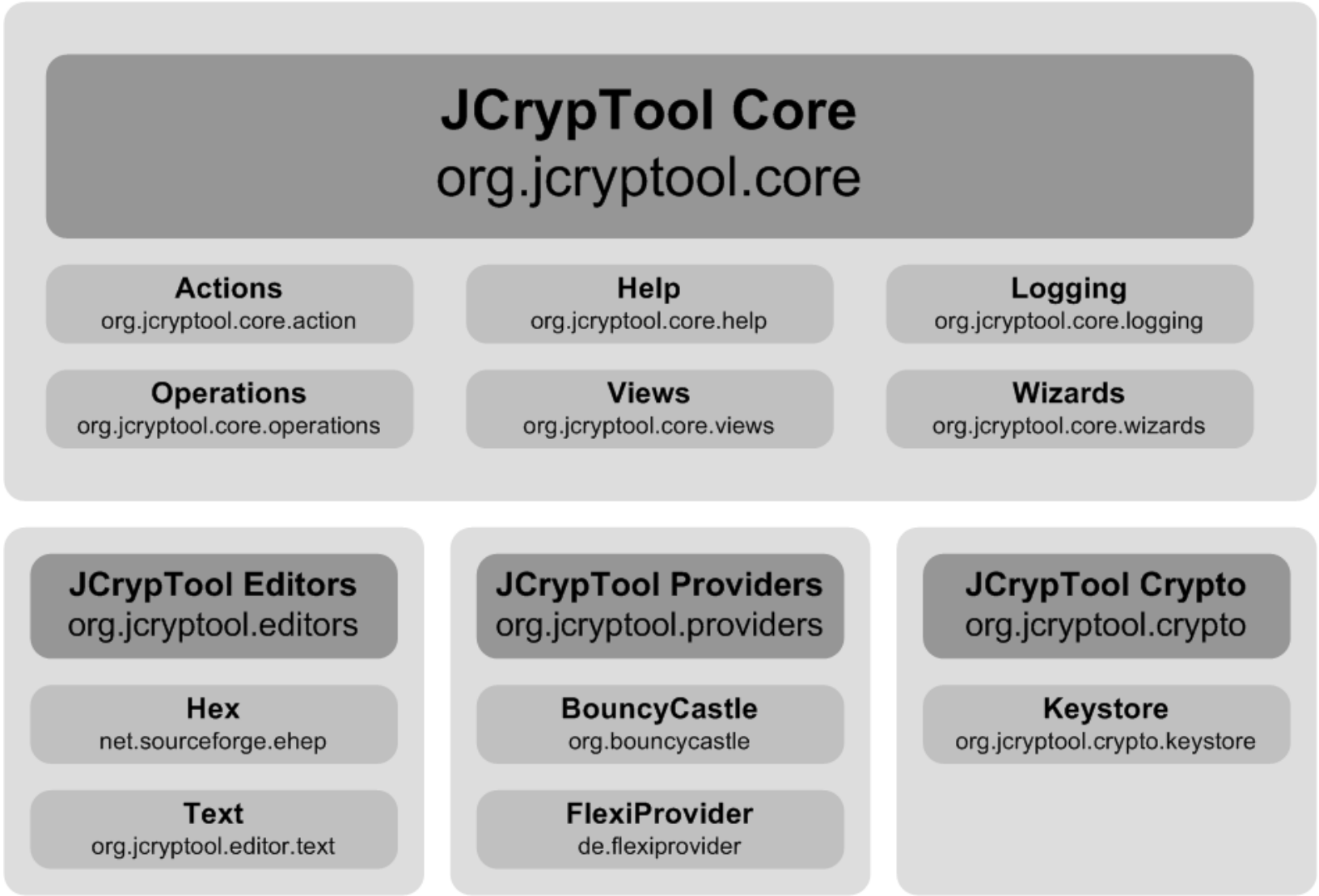
- **highly extensible**, easy to develop your own crypto plug-ins
  - new type of e-learning software
  - we provide the platform, crypto plug-ins are up to the public
    - → **developers only have to focus on their cryptographic logic**

Overview (Core Project)

- 4 members in the core project
  - additional support by the well-known CrypTool project and the Technische Universität of Darmstadt
- delivers the **bare runtime** (includes **FlexiProvider** and all the modern crypto offered by FlexiProvider directly)
- core project provides
  - **editors** (hex, text, *xml*)
  - **crypto providers** (FlexiProvider, BouncyCastle)
  - basic **views** (algorithms, file navigator)
  - **update site**
  - **help**, **welcome page**
  - logging

http://sourceforge.net/projects/jcryptool

Overview (Core Project)



Overview (Plug-ins Project)

- 6 members → **the community**
- delivers the **crypto plug-ins**, depends on JCT Core
- **classic**, **modern** and **hash** algorithms
  - ADFGVX, Caesar, Playfair, Substitution, Transposition, Vigenère, …
  - AES, RSA, RSA-AES-Hybrid, Elliptic Curves, …
  - MD5, SHA-1, SHA-2, Whirlpool, …
- **games**, **visualizations**
  - NumberShark (also called “taxman game” in the US)
  - Huffman, Zero Knowledge

http://sourceforge.net/projects/jctplugins

Overview (Plug-ins Project)

Classic Algorithms
org.jcryptool.crypto.classic

- **ADFGVX** org.jcryptool.crypto.classic.adfgvx
- **Caesar** org.jcryptool.crypto.classic.caesar
- **Playfair** org.jcryptool.crypto.classic.playfair
- **Substitution** org.jcryptool.crypto.classic.substitution
- **Transposition** org.jcryptool.crypto.classic.transposition
- **Vigenère** org.jcryptool.crypto.classic.vigenere
- **XOR** org.jcryptool.crypto.classic.xor

Modern Algorithms
org.jcryptool.crypto.modern

- **AES** org.jcryptool.crypto.modern.aes
- **PKCS7** org.jcryptool.crypto.modern.pkcs7
- **RSA** org.jcryptool.crypto.modern.rsa
- **RSA AES** org.jcryptool.crypto.modern.rsa-aes

Games
org.jcryptool.games

- **NumberShark** org.jcryptool.games.numbershark

Hash Algorithms
org.jcryptool.crypto.hash

- **MD5** org.jcryptool.crypto.hash.md5
- **SHA-1** org.jcryptool.crypto.hash.sha1
- **Whirlpool** org.jcryptool.crypto.hash.whirlpool

Visualizations
org.jcryptool.visual

- **Huffman** org.jcryptool.visual.huffman
- **Zero Knowledge** org.jcryptool.visual.zeroknowledge

Overview (Plug-ins Project)

- **plug-ins project is open to anybody**
  - not limited to e-learning plug-ins (e.g. mail plug-in for encrypted/signed emails, …)
- some JCT rules to follow (as less as possible)
  - naming conventions
  - style guide
  - **extension points**

  } documented in wiki/ help
- required know how
  - Java
  - Eclipse plug-in development
  - cryptography ☺

http://jcryptool.wiki.sourceforge.net

Agenda

- Overview
  - Core Project
  - Plug-ins Project
- Demo
- Summary

Demo

Agenda

- Overview
  - Core Project
  - Plug-ins Project
- Demo
- Summary

Summary

- **Milestone 2** end of **June**: for developers and end users
- Milestone 3 end 2008, **final version 1.0.0 in 2009**
- interesting for **developers** and „normal“ **users**,
  focus moving toward end users
- planned features/ ideas
  - **XML Security**
  - **digital signatures**
  - **entropy** education (for texts from different languages)
  - a demo of KI algorithms for **cryptanalysis**
  - **S/MIME-PGP** comparison
  - multi-partite **key exchange** and **key agreement** (Eindhoven)
  - **help** (the theoretical part)
  - …

Summary

- the JCrypTool core team provides
  - the platform
  - forum, wiki, mailing list
  - general support and know-how
- the rest is up to **volunteer developers**
  - but e.g. Bernhard Esslinger gives assistance in cryptographic questions and can be a co-evaluator for thesis works students do at their universities
- **The first extensible e-learning platform, be a part of it!**

http://jcryptool.sourceforge.net

Thank you!