


# JCrypTool

The logo for JCrypTool features the text 'JCrypTool' in a white, sans-serif font. To the right of the text, there are several white arrows of varying lengths and directions, some pointing right and some curving upwards, set against a background of horizontal dotted lines.

The cryptography e-learning platform.

Thorben Groos, Simon Leischnig, Dominik Schadow

# Agenda

JCryptTool Basics

JCryptTool 1.0

Outlook

# Agenda

JCryptTool Basics

JCryptTool 1.0

Outlook

# JCrypTool Basics



## Based on Eclipse Rich Client Platform (RCP) and Java

- Available for all major platforms in 64bit - Linux, macOS, Windows
- Transparent for the developer (in theory)
- Common limitations of the Eclipse IDE, look & feel is challenging for non-developers

## Platform independent plug-ins

- Completely extensible with plug-ins (everything is a plug-in)
- Learn and develop cryptography - everyone can develop an own plug-in
- High barriers to entry for developers - Eclipse RCP is not that common any more

# Complete Extensibility with Plug-ins

## Core

- More than **20** core plug-ins
- Providing common functionality like editors (text and hex), views (log, keystore, file and algorithm navigators, ...), keystore services (BouncyCastle and FlexiProvider)
- Fall-through hierarchy of crypto providers
- Multi-language support (currently German and English)

## Crypto

- More than **60** crypto plug-ins
- Analysis, classic and modern algorithms, games and visualizations
- From relatively simple algorithms to complex visualizations

# Facts and Figures

## Keeping everything up-to-date (technologies and tools)

- Started on SourceForge (SVN), moved to GitHub (Git)
- Release builds on TravisCI - fully automated weekly builds
- Updating:
  - Eclipse RCP is relatively easy - we switch to every new version
  - Java is (now) more challenging - moving away from Java 8 now

## More than 50 contributors

- From one-time contributors, students and student teams to regulars
- Divided into core and crypto teams - with read only or write access

# Attracting Developers

The screenshot shows the GitHub repository page for `jcryptool / core`. At the top, there are navigation links for Code, Issues (18), Pull requests (0), Projects (1), Wiki, Security, Insights, and Settings. On the right, there are buttons for Unwatch (19), Unstar (79), and Fork (27). Below the navigation is the 'Home' section, which includes a 'New Page' button and a note that Thorben Groos edited this page on 8 Jul with 88 revisions. The main content area is titled 'Welcome to the JCryptTool Wiki!' and contains three paragraphs of introductory text. To the right of the main content is a sidebar with a 'Pages 38' header and a list of links: Home, Main Page, Project Ideas, Project Ideas, Developers, Documentation, Getting Started, Coding Conventions, and Users.

`jcryptool / core` Unwatch 19 Unstar 79 Fork 27

<> Code Issues 18 Pull requests 0 Projects 1 Wiki Security Insights Settings

Home Edit New Page

Thorben Groos edited this page on 8 Jul · 88 revisions

## Welcome to the JCryptTool Wiki!

Our wiki contains the latest and most important information for **JCryptTool Core** and **JCryptTool Crypto** developers and can be extended with information by any project member.

This wiki is intended for plug-in developers. Basic information for end-users on using JCryptTool functionality is available in the **User Guide** section in the JCryptTool help included in every release.

**Need more help?** Join us in our [Gitter Channel](#) (our preferred way of communication). We will be happy to assist you with any problem or question you might have!

## Project Ideas

Interested in developing a plug-in for JCryptTool and in becoming part of the growing JCryptTool

Pages 38

- Home
- [Main Page](#)

Project Ideas

- [Project Ideas](#)

Developers

- [Documentation](#)
- [Getting Started](#)
- [Coding Conventions](#)

Users

More than 25 source **code forks**

Public **wiki** with getting started guides, technology information, some common requirements, style guides, and release planning

**Gitter** channel

Public **issue tracker** for core and crypto

Approaching release **1.0.0** -- more on that by Thorben Groos

# Agenda

JCrypTool Basics

**JCrypTool 1.0**

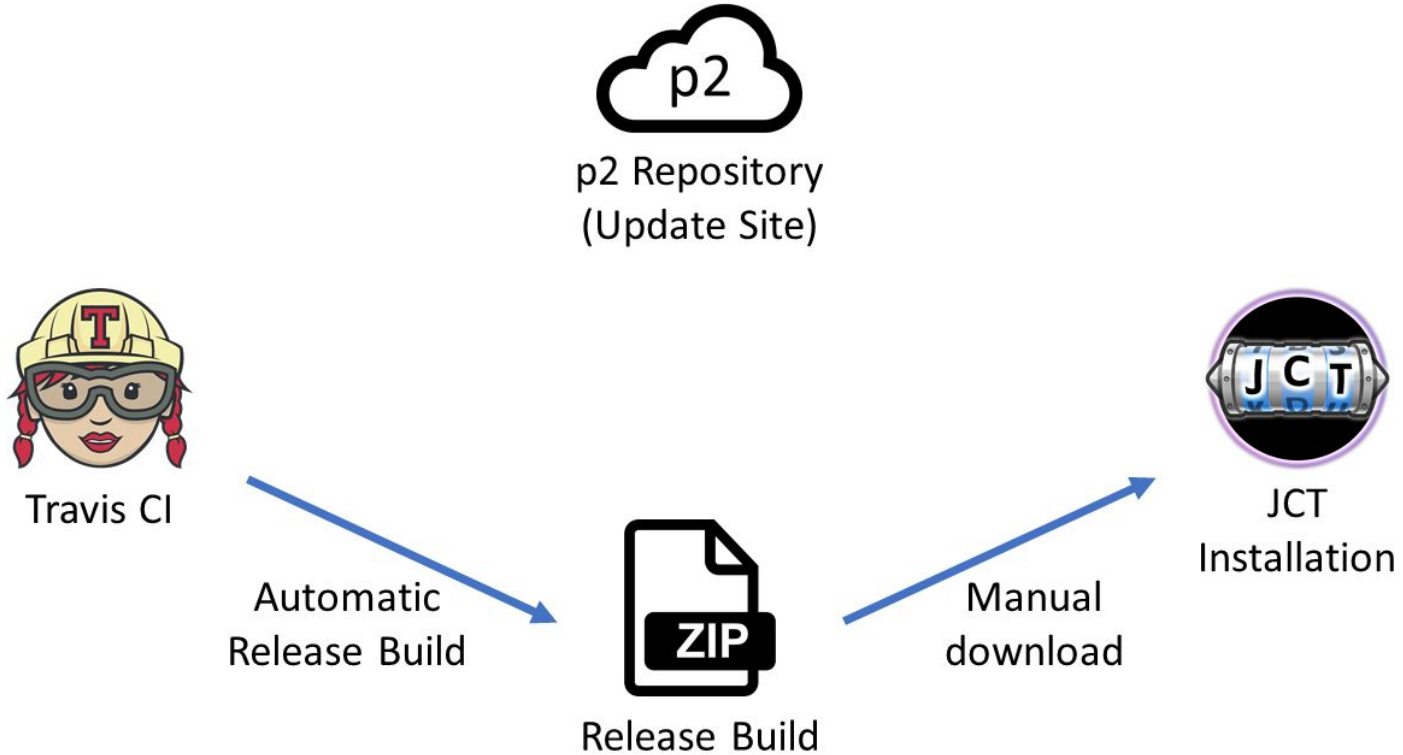
Outlook



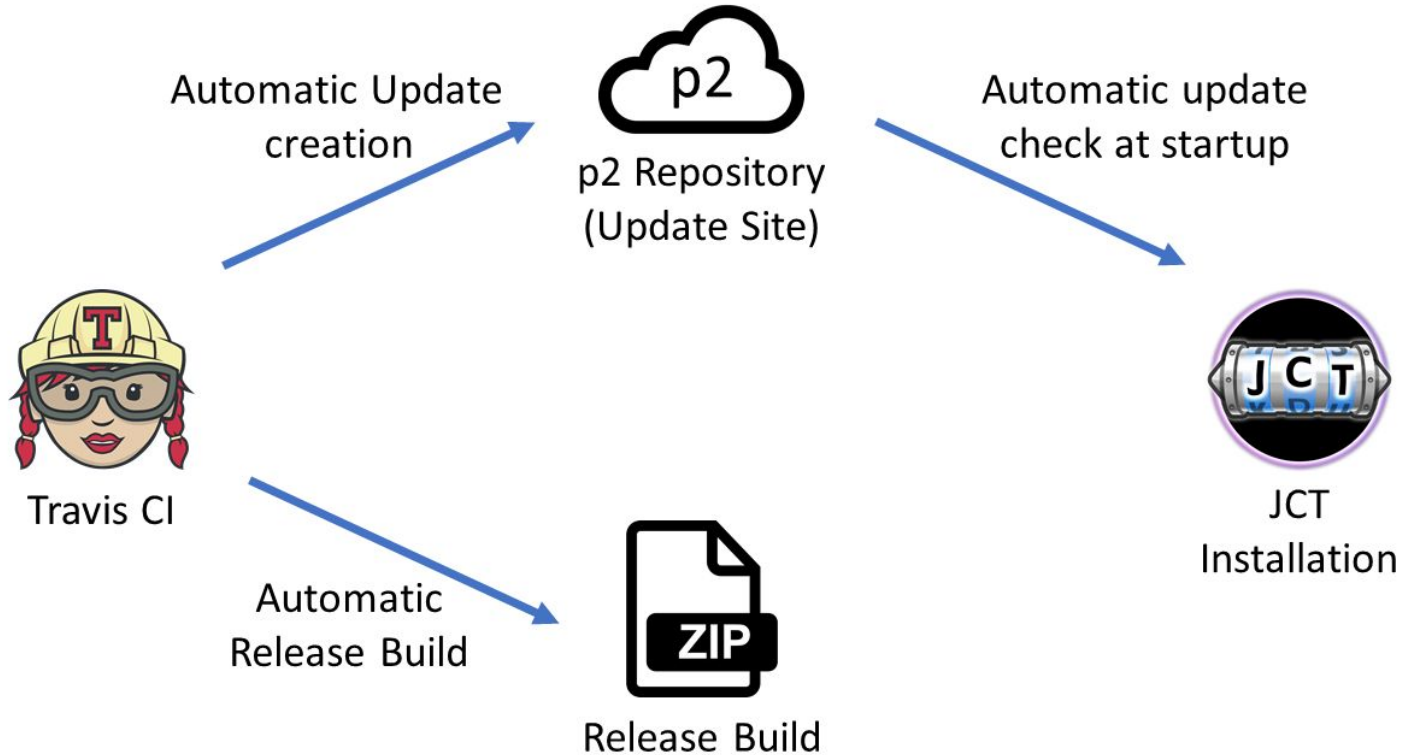
# What's new in JCrypTool 1.0

- Completely available in German and English
- 2 new plug-ins: SPHINCS+ Signature visualization and Grille analysis
- New update process
- JCrypTool - JRE - Bundle
- GUI improvements and bug fixes

# Update Process - conventional



# Update Process - via a provisioning platform (p2)



# JCrypTool-JRE-Bundle

- Migrating from Java 8 to Java 11
- We ship a Java 11 JRE with JCrypTool 1.0

**Advantage:** No installed JRE is needed anymore to run JCrypTool

# Agenda

JCryptTool Basics

JCryptTool 1.0

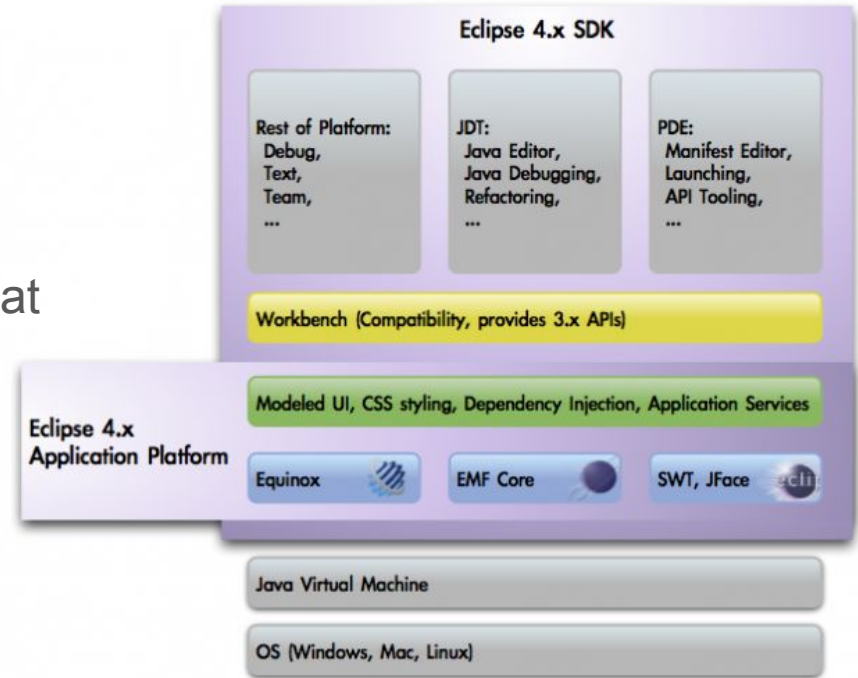
Outlook

# Outlook

1. Eclipse E4 Migration
2. BouncyCastle und JCrypTool
3. Build process improvements

# Eclipse 4 (e4) Migration

- Future-proof JCrpTool
- Currently: compatibility layer
- Multi-stage migration:
  - core
  - common prototypes & own compat
  - batch



# BouncyCastle and JCT

- BouncyCastle: APIs for cryptography  
<https://www.bouncycastle.org>
- Many modern algorithms included
- Challenge: Generic UI model
- Goal: JCT as GUI for BouncyCastle





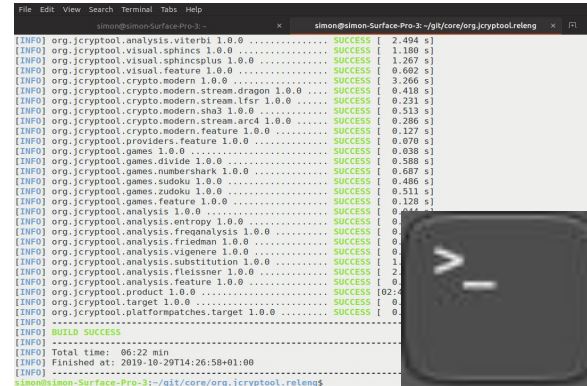
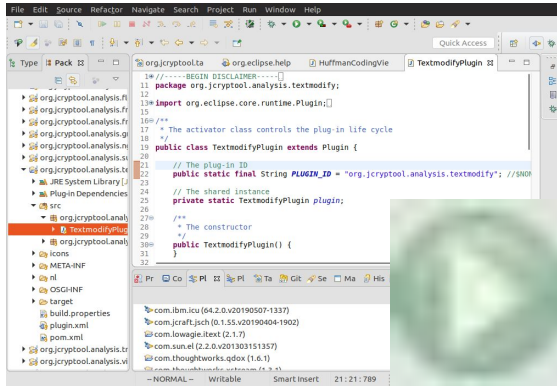
# Build Process

“Developer Build” is not “Release Build” !

Target Platform

Developer Build (Eclipse PDE)

Release Build (Maven/Tycho)



# Build Process - New Possibilities

Through a new experimental project...

<https://github.com/simlei/org.jcryptool.thirdparty>

- Depend on libraries from Maven Central
  - `<dependency>{group:id:version}</dependency>`
- Load off heavy features (e.g. JRE)
- Patch the eclipse platform!

# Outlook

- **Big future projects:** E4 migration, BouncyCastle UI
- **Stable infrastructure** through further improving our build process

**Thank you**

<https://github.com/jcryptool>