JSR 321: Public Review

Java Community Process

January 2011

Ronald Tögl

IAIK – Graz University of Technology
ronald.toegl@iaik.tugraz.at

Trusted Computing API for Java™

Stage	Start	Finish
Public Review Ballot	*01 Feb, 2011*	*07 Feb, 2011*
Public Review	*03 Jan, 2011*	*07 Feb, 2011*
Early Draft Review	09 Apr, 2009	08 Jul, 2009
Expert Group Formation	11 Dec, 2007	31 Jul, 2008
JSR Review Ballot	27 Nov, 2007	10 Dec, 2007

Contact us:

➔ http://jsr321.dev.java.net

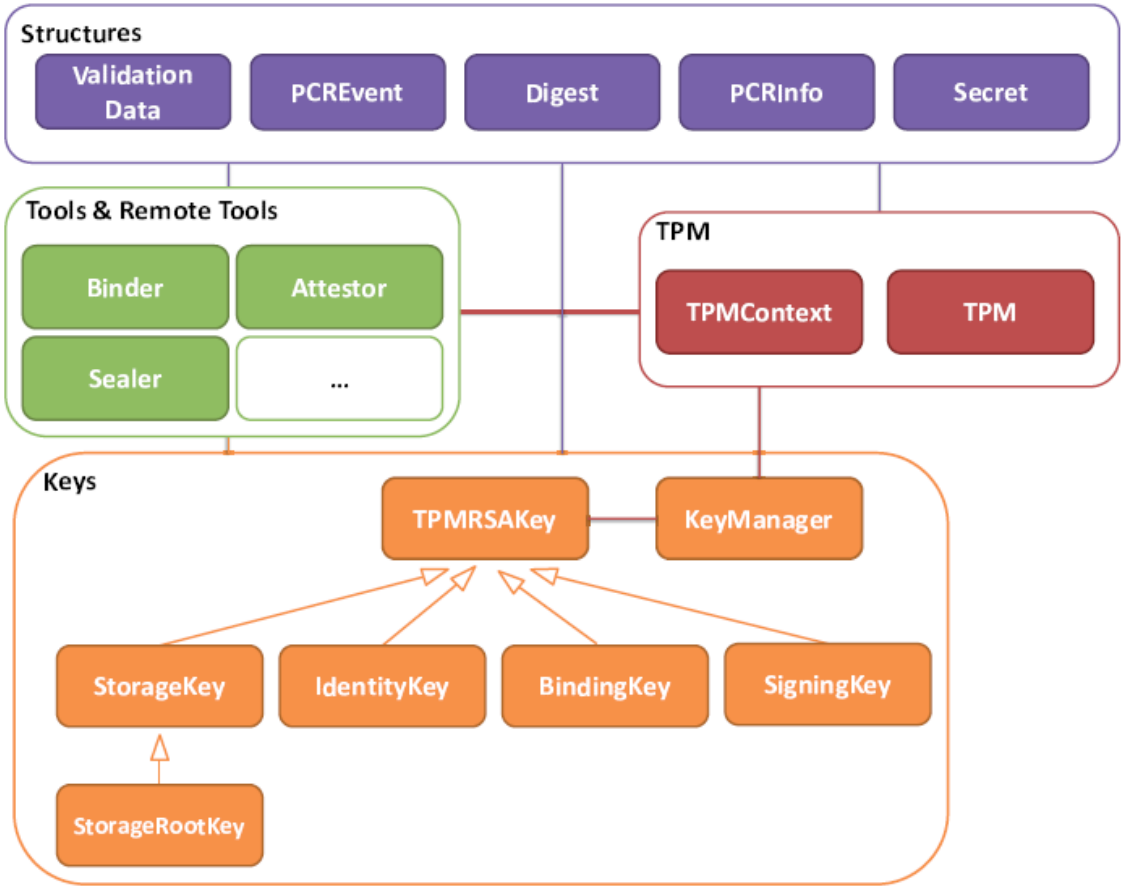
➔ eg@jsr321.dev.java.net

Since Early Draft Review

- Received comments from industry and academia: IBM, StrongAuth, Postilion, Univ. Birmingham,..
- EG also received extensive input by a completely **independent implementation** of the EDR API (using C++) by ATEGO for the European FP7 project TECOM

API Overview

`javax.trustedcomputing.*`



Changes to API

- Class `TPM`
  - `public Object getProperty(String property);` instead of multiple getter Methods
  - moved `quote()` to new Attestor tool.
- Class `TPMContext`
  - Implementation can now be defined at runtime or via `jsr321.tpmcontextimpl` property
- New Class `PCRsNotAccessibleException`
  - Thrown if OS blocks selected TPM ordinals (default configuration of Windows)

Changes to API II

- Package `tools`
  - New Class `Attestor` for Remote Attestation
  - `Initializier` (optional) for initalizing the TPM if functionality is not provided by OS (Linux)
  - `Certifier` to sign and verify key policies
  - `TickStamper` was removed as abstraction from TCG standards proofed difficult

Changes to API III

- Package `tpm.structures`
  - Now also allows public construction of structures where useful
  - Class `ValidationData` made serializable
- New sub-package `tpm.tools.remote`
  - For functionality that does not require a local TPM (i.e. to implement security protocols)
  - New Classes that help with analysis and validation:
    - `RemoteAttestor`
    - `RemoteBinder`
    - `RemoteCertifier`
    - `RemoteSigner`

Further Decisions

- `javax.trustedcomputing.*` package name describes the content of JSR 321 better than abbreviations
- Final software license for API, RI, will be *GPLv2 with Classpath Exception*.
- IAIK is currently completing and updating RI, TCK