

Java Cryptography Provider for Trusted Platform Modules

Motivation:

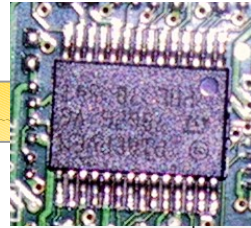
Most of today's business class desktop computers and notebooks are equipped with Trusted Platform Modules (TPMs). These TPMs provide smart-card like functionality, including key management and signature generation. On the software side TPMs are accompanied by a rather large and complex software stack. On the contrary, Java has a well-documented, established and easy to use cryptography framework. One of the outstanding features of the Java Cryptography Architecture is the possibility to plug-in own providers for algorithms and cryptographic tokens.

Project description:

The goal of the project is to design and implement a Java Cryptography Provider which provides selected functionality of the TPM to Java applications through the standard Java cryptography framework. The TPM functions provided to the Java environment will include signature generation, sealing and binding.

Tasks:

- Design and implement a Java Cryptography Provider for the TPM
- Implement the signature and quoting facilities of the TPM on top of the JCA
- Investigate methods to integrate TPM binding and sealing facilities into the JCA



```
import java.security.Signature;
import java.security.PrivateKey;
...
public class TpmSignatureDem
{
    public static byte[] sign(byte[] data,
        PrivateKey key) throws SecurityException {
        Signature sig = Signature.getInstance(
            "SHA1withRSA", "TPM");
        sig.initSign(key);
        sig.update(data);
        return sig.sign();
    }
}
```

Master Project

Participants: 1-2 Students

Prerequisites:

- Experience with C & Java software development
- Basic understanding of cryptography and Trusted Computing

Contact:

Kurt.Dietrich@iaik.tugraz.at
Johannes.Winter@iaik.tugraz.at

Studies: INF SEW TEL Master Thesis

The master project can be continued as master thesis.