2016-10-11

Master Thesis

Blockchains in Distributed PKI Solutions

Background
PrimeKey is looking for one or more students to investigate how blockchain technology can be used for large scale distributed PKI solutions.

PKI solutions are traditionally relying on very strict deterministic and synchronous transactional behavior, where a transaction is to issue a certificate to an end entity (user, device, server etc) and ensuring the recording of this certificate for validation purposes (verifying that the certificate was in fact issued and that it has not been revoked). In the hyper scale world of cloud and IoT this sometimes poses challenges to maintain a globally distributed, redundant, PKI infrastructure with high availability and robustness, while preserving short latencies. The advent of blockchain technology comes with a lot of hype and promise of disruption in the traditional transaction based industry. Identity management and PKI are also challenged, so far without serious alternatives using blockchain, but there are new and interesting use cases where a blockchain based approach may have advantages. There are multiple ways blockchain technologies can be used coupled with PKI:

- Hybrid; where transactions are done on a blockchain, and identity is managed in a class PKI, and these are connected.
- Pure blockchain based; where the PKI relies on blockchain technology instead of traditional transactional databases.

Blockchain is in reality a collection of different technologies and implementations, all with different characteristics and thus suitable for different use cases. PKI based use cases typically require large scale and short transaction times. In order to use blockchain technology for PKI solutions, one might have to take a more probabilistic approach instead of the traditional deterministic approach.

Thesis Description
The thesis would consist of several parts:

1. Investigation of existing and upcoming blockchain technologies to find out what the benefits and drawbacks are with different blockchain technologies. What are the deterministic vs probabilistic characteristics?
2. Investigation and suggestions how a hybrid approach can be modeled and how PKI based identiy can be tied into transactions on the blockchain to support non-anonymous usage.
3. Modelling and proof-of-concept of a blockchain based PKI solution using the best suited blockchain technology from the first investigation.

Student Profile
You are probably a Master of Science student in electrical, computer or physics engineering. You are most likely interested in one or more of the following areas: Computer science and algorithms, PKI, mathematics, databases and IT security. If you also happen to enjoy Java, Linux and open source software this is definitely the place for you!

Highly valued personal qualifications and competencies are as follows:

- Driven and action-oriented
- Ability to work independently, proactively and responsibly
- Ability to take own initiative
- Structured and organized
- Positive and easy to co-operate with others

Location
PrimeKey HQ in Solna, Stockholm, Sweden

Application and Preferred Starting Date
We look forward to receiving you application no later than 25:th of November. Interviews will be held continuously and preferred starting date is as soon as possible.

Further Opportunities
PrimeKey is growing and we are continuously looking for skilled people to join our team. A successful Master Thesis project is an excellent way to get to know us! Are you up for the challenge?

For More Information
Please contact Magnus Andrén, VP Engineering, PrimeKey Solutions, magnus.andren@primekey.se or PhD Student Jonathan Jogenfors, ISY, Linköping University, jonathan.jogenfors@liu.se

ABOUT PRIMEKEY
PrimeKey Solutions AB is one of the world's leading companies for PKI solutions. PrimeKey has developed successful solutions, such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation. PrimeKey has its head office in Stockholm, offices in Aachen, and partners in Kuala Lumpur, San Mateo and Washington D.C. Clients in Sweden include Bankgirot (Sweden's only clearinghouse) and the Swedish Police (issuing passports and national ID cards to Swedish citizens).