Master Thesis Proposal

Agile PKI

Background
PrimeKey is looking for one or more students to investigate a scheme for how established, large scale PKI installations can migrate algorithms.

PKI is currently the primary technology for protecting communication and documents, through asymmetric encryption and digital signatures. Asymmetric cryptography is based on mathematical problems that are very hard to solve using today’s computers, yet the constraints of today’s computing power doesn’t allow for algorithms that are secure against tomorrow’s. In the short term we’re already seeing this with ever growing key sizes and more complex hash algorithms, such as SHA3 which will in time become the industry standard.

While current standards allow for key sizes to evolve by limiting the lifetime of certificates (giving opportunity to update them using new keys), changing the signing algorithm of a PKI isn’t quite as simple. In the medium to long term, traditional algorithms such as RSA and EC are going to have to be replaced entirely by quantum-safe algorithms, in anticipation of the first Quantum computers becoming operational.

What the industry currently lacks is a method for actively migrating a PKI environment from one signing scheme to another without downtime or a noticeable performance degradation. Adding to the complexity is the fact that apart from the central issuing system, also relying parties verifying signatures must be able to verify signatures in order to operate correctly.

Thesis Description
The thesis would consist of several parts where the most important ones would be:

1. Investigation a method for migrating existing CA's from one signing scheme to another.
2. Investigation a method for migrating existing CA's from current signing algorithms to quantum safe algorithm
3. Investigate the possibilities to add new algorithms to a PKI software without requiring extensive re-programming.
4. Developing a proof-of-concept for migrating a CA according to the above.

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 your application no later than 31:th of January. 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.com

ABOUT PRIMEKEY
PrimeKey Solutions AB is one of the world's leading companies for PKI and digital signing solutions. With our products EJBCA, SignServer and the PKI Appliance, we deliver the capability to implement an enterprise grade PKI system ready to support solutions such as IoT, e-ID, e-Passports, authentication, digital signatures, code signing, digital identities, and validation; all solutions where digital certificates would be a main enabler.

Delivered on-prem or in the cloud, our products are used in all type of industries where IT security and integrity is a priority. Our products are Common Criteria and FIPS certified, we have numerous Webtrust/ETS1 and eIDAS audited installations, and our internal processes are ISO 9001, 14001, and 27001 certified.

PrimeKey has offices in Stockholm, Sweden; San Mateo, USA; and Aachen in Germany. Together with our global network of technology and resell partners we are proud to count many of the industry leading companies and institutions within IT, Telecom, Banking, Industrial, Public CAs, and different branches of Government as our long-time customers.