PrimeKey

Call for speakers **PrimeKey Tech Days 2018**

This is a list of suggested topics that we would like to address during PrimeKey Tech Days 2018. If you have an idea that is of relevance but not on this list – please reach out to us and we will take it under consideration.

Foundation

- Core PKI and core crypto – technologies that enable us to implement PKI products for multiple use cases. Without proper foundation, say implementation of random number generators, to unambiguous coding of ASN.1 structures, we are neither secure nor interoperable. Slight preference to Java related topics.
- Public CA and Certificate Transparency – is the green lock on EV certificates just a fake security sold by Public CAs? What are the alternatives that can work and scale? Certificate Transparency in 2018?
- Hardware Security Modules – we want to hear how HSM vendors and users think about state of the art and future. We suspect that HSMs will enter a transformational phase due to new requirements and new technologies - from quantum crypto and agile cryptography to cloud HMS and trusted execution environments as alternatives to traditional form factors.

Practice

- Use cases for PKI – we love to hear how organizations use PKI, ranging from multiple use cases, to large scale deployment or critical infrastructure. Very often is it practitioners that point at deficiencies in products or standards. What problems in implementation or in operations were experienced and how they were solved?
- Security of/for IoT – small preference here on Industrial IoT use cases and situations where IoT is not yet-another-PKI-deployment. For instance, we would love to hear about “birth certificates” or supply chain implications on requirements and implementation of robust IoT solutions.
- Security for DevOps, Microservices and other new cool things – is REST a must-have and if so, what else is needed to provide seamless automation of PKI related services that enable deployments and use in modern architectures? What about short-lived throw-away certificates, for instance?
- Security protocols & standards – What is new and of relevance in standards? How are we doing with EST? MPKAC is a promising idea to allow migration to quantum safe signature schemes. We are open to hear also limitations of existing standards, or suggestions for new things – here is crazy example - REST enabled PKCS#11?
- CodeSigning – some vendors learn about importance of code signing only when their signing keys get stolen. We would like to hear examples of how to do it right with code signing? Are there perhaps too many standards for code signing or what are deficiencies experienced in real life usage?
- Document signing / eIDAS – both within and outside of EU, document signing has become a big business. Not surprise, since when done well it can save tons of money for business and public sector. We would like to hear how is going in EU, with eIDAS regulation being in place, but also how is going in other parts of the world.

Future

- Agile Crypto / Agile PKI – threat of quantum computers brought attention to cryptographic agility, but this is not the only reason – there is an elephant in the room – consider migration efforts when a new standard is introduced. Is there an agile crypto that will upgrade us to whatever is the state of the art? How about PKI in particular? Is it even realistic to assume we can create an agile PKI unless there is a plethora of new standards both for client and server side?
- Quantum Safe Cryptography –What is the state of the art in 2018 and what are the best available predictions? Looks like we will end up having different classes of algorithms for different purposes. Is there a hope for classical crypto to survive?
- Blockchains – great about promises on revolution but we feel it still may be more hype than general usability - is there something that is standardized, running and robust enough? If not quite yet, what could be good candidates?

Contact PrimeKey

The speaker agenda is already starting to fill up, so please submit your interest as soon as possible. Read more about the event at www.primekey.com/tech-days

Submit your interest to: techdays@primekey.com