PrimeKey

Call for Speakers
PrimeKey Tech Days 2020

Stockholm, Sweden
September 15th & 16th, 2020

These are suggested topics that we would like to address during PrimeKey Tech Days 2020. If you have an idea that you think is of relevance but is not on this list – please reach out to us and we will take it under consideration.

Please note the deadline for submission of your abstract is April 30th, 2020. We will confirm acceptance by May 15th, 2020.

Foundation

- **Core PKI and Core Crypto**

  Enabling technologies for implementation of PKI products that are usable in multiple use cases. Without proper foundations from, say, random number generators, side-channel-safe implementations of crypto algorithms, or unambiguous coding of ASN.1 structures, we are neither secure nor interoperable. Preference to Java-related topics.

- **Public Trust and Audits**

  State of the union for publicly trusted certificate in 2020 – is trust rock solid? What are the new initiatives and requirements about code signing, network security, server certificates from CA/B forum? How will collaboration between industry associations and organizations (such as ETSI and CABF) benefit enterprise users? Are audits providing the value they should?

- **Hardware Security Modules**

  What HSM vendors and HSM users think about future developments and state of the art technology of HSM? We see HSM vendors offering cloud-like services, support for quantum-safe cryptography, or multi-party computing based on virtual HSMs. How is it going with adoption of PKCS#11 v3 in HSM? Are the implementations in trusted execution environments proving to be good alternatives to traditional form factors?

- **Standards and Compliance**

  What technologies are new or updated that affects PKI products or PKI deployments? Is the BRSKI (Bootstrapping Remote Secure Key Infrastructures) the hottest thing for IoT? What about Cybersecurity Act? Some examples we are interested to hear from you – is PKCS#11 v3 going to deliver the improvements we need, and are vendors delivering to your expectations? We would also like to review limitations of existing standards, or suggestions for improvements.

PKI in Practice

- **Use Cases for PKI**

  Our attendees favorite since this topic brings both implementors and practitioners. We would like to hear how organizations use PKI, ranging from multiple use cases (email encryption, intranet TLS, Active Directory login, 802.1x, VPNs, etc.), to large scale deployments (performance and/or scale requirements) or critical infrastructure (“everything” stops working if the PKI is down). Where and how are cloud deployments working? Very often it is the practitioners that point at deficiencies in products or standards! What challenges were experienced during integration, implementation or in operations and how were they overcome?

- **IIoT Security and OT!**

  What are the best processes to deliver PKI to secure IoT/IIoT deployments? Recommendations for Industrial IoT use cases and integrations, such as IoT platforms and other infrastructures that enable digital transformation of manufacturing. How well we address needs from Operational Technologies? What are the supply chain requirements to deliver robust and secure IoT solutions? Are the standards ready for manufacturers to lean on, such as ISA/IEC 62443**,** or NIST / ENISA guidelines?

- **Security for DevOps, Microservices and Emerging Technologies**

  Are containers what everyone will run? How well do you find containers work with PKI? Issuing certificates to containers, code signing and signed containers? What else is needed to provide seamless automation of PKI related services that enable deployments and uses in modern architectures? What about short-lived throw-away certificates for instance?

- **Security Protocols**

  As we suggested in 2019, it is clear that ACME got significant traction, but EST and even CMP is alive and well. What is cool and what is cumbersome? What else is new and of relevance in protocols used to implement PKI in real-world scenarios? We are in particular interested in use cases that demonstrate automation and can scale well.

- **Code Signing**

  Some vendors learn about the importance of code signing only when their signing keys are stolen. We would like to hear recommendations and examples on how to do it right with code signing? Are there too many standards for code signing? And what are the deficiencies experienced in real life usage?

- **Document Signing / eIDAS**

  Both in and outside of the EU, document signing has become big business. It's no surprise that seamless document signing saves money for the business and public sectors. With the eIDAS regulation in place in the EU, we would like to hear about any impacts to the EU and other parts of the world. Are the eSeal and PSD2 the most important use cases that we should focus on?

Future

- **Agile Crypto / Agile PKI**

  The 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 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 the client and server side?

- **Quantum Safe Cryptography**

  What is the state-of-the-art quantum safe cryptography in 2020 and what are the best available predictions? Most likely there will be different classes of algorithms for different purposes. Is there hope for classical crypto to survive?

Contact PrimeKey

The speaker agenda is filling up fast, 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