PrimeKey

Call for Speakers PrimeKey Tech Days 2021

Stockholm, Sweden
September 14th & 15th, 2021

We are delighted to invite you to consider presenting at PrimeKey Tech Days 2021. Here are suggested topics and questions that we would like to address during PrimeKey Tech Days 2021. 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, 2021. We will confirm acceptance by May 21st, 2021. Presentation time is set to be 25 minutes. PrimeKey will help record your presentation, but we hope you can be available online for questions and answers during the Tech Days.

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.

- Public Trust

  State of the union for publicly trusted certificate in 2021? 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 ESTI and CABF) benefit enterprise users?

- Hardware Security Modules

  What HSM vendors and HSM users think about future developments and state of the art technology of HSM? We see major HSM vendors offering cloud-HSM services, support for quantum-safe cryptography, and multi-party computing based on virtual HSMs. How is it going with adoption of PKCS#11V3 and how are other HSM APIs being used? How is it going with eIDAS-related certifications? Are the implementations in trusted execution environments proving to be good alternatives to traditional form factors?

- Standards and Compliances

  What technologies are new or updated that affects PKI products or PKI deployments? Where are we with eIDAS standardization and adoption? What about CyberSecurity Act? Some examples we are interested in hearing from you – is Common Criteria still delivering valuable quality and security and are vendors delivering to users' expectations? We would also like to review limitations of existing standards, or suggestions for improvements.

PKI in Practice

- Use Cases for PKI

  Our attendees like this topic since it brings together 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 cloud and hybrid deployments (performance and/or scale requirements) or critical infrastructure ("everything" stops working if the PKI is down). 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

  What are the best practices to deliver PKI to secure IoT/IIoT deployments? How some verticals, for instance transportation sector, think about and adopt IIoT Security? 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 containers? What else is needed to provide seamless integration and automation of PKI related services that enable deployments and uses in modern architectures?

- Security Protocols

  What 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. Are there some updates with quantum-safe algorithms, and what are implications for users?

- 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? What are your experiences with code signing? We are also keen to hear about RedHat's new code signing with built-in transparency.

- Document Signing

  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 eIDAS regulation in place in the EU, we would like to hear about any impacts to the EU and other parts of the world. We would like to see cool implementations with integrated document management workflows.

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 2021 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