Everything You Didn't Want to Hear about PKI and SHAKeN/STIR

SIPNOC 2019

December 4, 2019

MARK B. COOPER
PRESIDENT & FOUNDER

MARK@PKISOLUTIONS.COM
@THEPKIGUY

PKI SOLUTIONS

The PKI Guy

- President and Founder, PKI Solutions
- Known as “The PKI Guy” since early days at Microsoft
- Leading PKI and SHAKEN/STIR subject matter expert
- At PKI Solutions, we implement PKI solutions at enterprises
- I lead hundreds of PKI trainings from Scotland to Buffalo, Sweden to Portland
- In-person and online trainings available
- My focus is security, PKI design and implementation, identity management

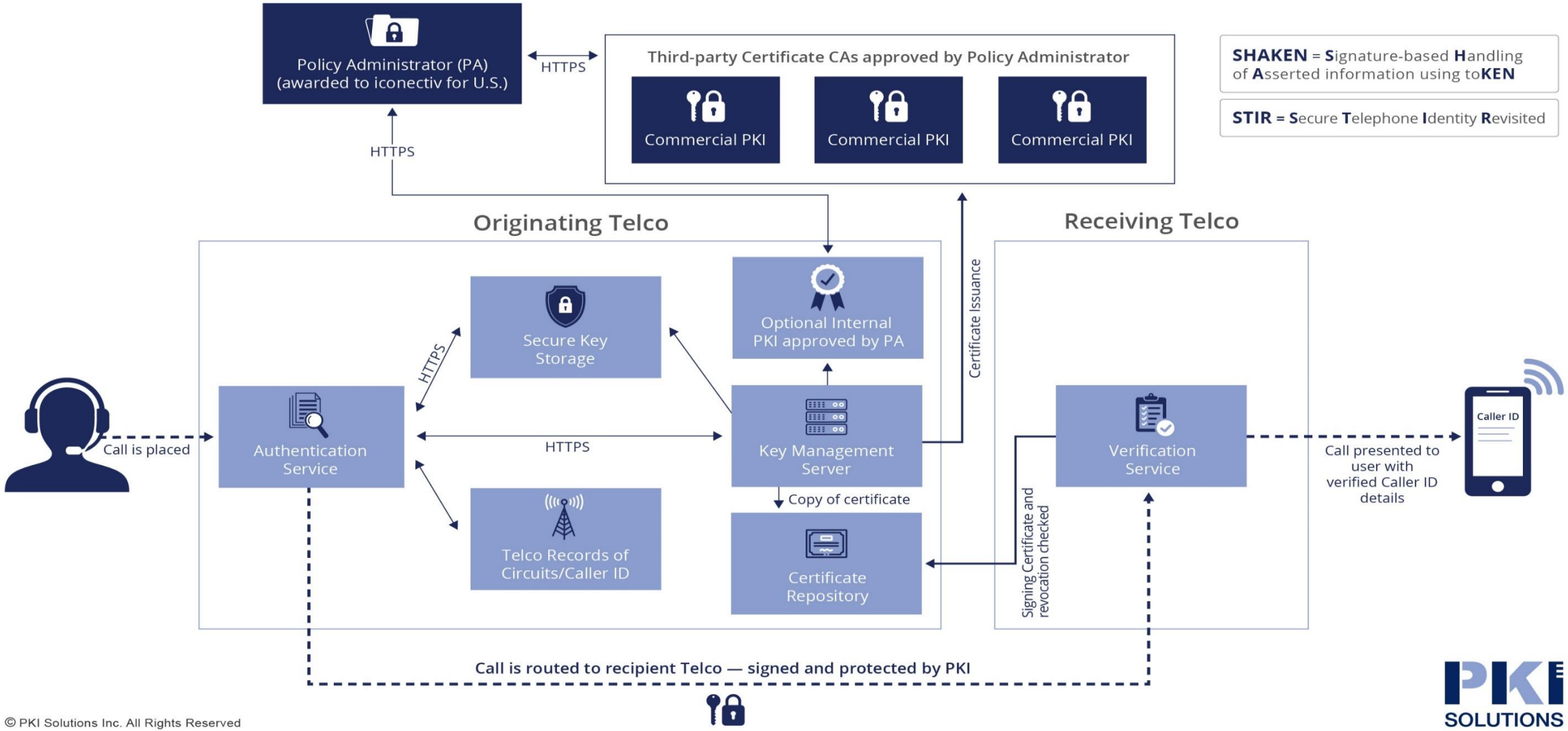
PKI SOLUTIONS

PKI is at the Core of SHAKeN/STIR

PKI SOLUTIONS

- Public key infrastructure (PKI) is the backbone of SHAKeN/STIR
- PKI used to identify and verify each phone call
- SHAKeN/STIR uses digital certificates, based on common PKI cryptography techniques
- Ensures the calling number of a telephone call is secure
- Uses digital signatures at every single call, which are verified and authenticated
- SHAKeN/STIR shifts the identity details from the call originator to the telephone company
- Each telephone service provider obtains its digital certificate from a certificate authority that is trusted by other telephone service providers
- The certificate technology enables the called party to verify that the calling number is accurate and has not been illegitimately spoofed

Global SHAKEN/STIR Framework



PKI SOLUTIONS

Critical Needs to be Successful

- All carriers need to get on board
- Needs to be created with a trusted PKI system as the base
- Technology infrastructure, telecommunications, and government entities need to work together to ensure call identities are trusted globally
- Security required at every level
- Technical issues
- Must be addressed globally – bad actors will relocate to exploit weaknesses
- Standards need to be enforced through assessments and compliance

PKI SOLUTIONS

Unique Requirements for SHAKeN

- Indirect CRL – Signed by STI-PA CAs, not STI-CA
  - RFC 5280 Compliant, seldom used
  - API/Electronic notification to STI-PA
- Certificate eco-system for SHAKeN only, no other uses
- Certificate Repository
  - Uncommon in most PKIs, but essentially just HTTP
- ACME & Service Provider Code Token
- ECC Key Algorithm Only & SHA256 Hashes
- Commercial CA or Service Provider based Issuance

PKI SOLUTIONS

Overview to Commission a STI-CA

PKI SOLUTIONS

- Architecture/Design
- Certificate Practice Statement
  - Draft
  - Submission to STI-PA
- Security Controls, Auditing, Personnel
- Documentation and Workflow
- Deployment
- Piloting
- STI-PA Auditing?

STI-CA Considerations

- Nothing dictates a multi-tier PKI
  - **Not a recommendation**
- No Hardware Security Modules Required
- Relatively small CP to comply with (38 pages)
  - Security
  - Roles and Responsibilities
  - Facilities – Power, Air, Water, Data Retention, Access Controls
  - Background Checks, Training, Auditing, Incident Response & DR
- Considerably lower security and requirements than WebTrust
- Aligns with 95%+ of practices in place for Commercial CA
- SHAKeN requirements will require customized CA software

PKI SOLUTIONS

Uncertain Items in STI-CA Certificate Policy

- CPS Suitability and Assessment/Audits
- Trust process for STI-PA issued trust list
- Meaningful Names – but not too meaningful
- Interop with global SHAKeN ecosystem - Trusts

indirect

PKI Challenges

- Indirect CRL Customization requirements (API Notification, etc…)
- ACME & SPC Token Support
- Time consuming to create Certificate Practice Statement
  - Shouldn’t be aspirational – must be verified/auditable
- Financial viability for STI-CAs operating commercially vs internally
- Security must be cradle-to-grave.

Weaknesses and Exploits

- Extremely vulnerable to implementation exploits
  - Attested by originating telco: Adversaries move too slow to implement countries/telcos
  - Calls still go through unattested: Still accomplishes bad guy goals
- High value will be placed on compromising SHAKEN/STIR CA certificate/key
  - Compromised key will enable virtual switch to attest calls
  - No OCSP – detection of fraudulent/compromised keys unlikely
- PKI is tough
  - Assuming all telcos implement eventually, many will do so cheaply, quickly, or operate insecurely
  - 2,000 in U.S., only top 10 are of “considerable” size
- DOS attack will render attestation unverified, but calls persist
  - Could bypass blocking/flagging by receiving telco and user devices

PKI SOLUTIONS

Your PKI will be a Target

- STI-CA will be highly targeted for exploitation – direct financial gain
  - Dark web market for TLS certificates
- Minimal requirements around key control & lack of compromise detection of CA
- Software based keys are impossible to tightly control
- Software based keys are insecure (Heartbleed)
- Centralized STI-PA administrated/distributed trust list means latency during recovery
- Adversaries are internal and external to organizations
- SHAKeN/STIR integrity is highly contingent on security of the underling PKIs – around the world

PKI SOLUTIONS

Questions? Let's Connect!

mark@pkisolutions.com

@ThePKIGuy

@PKISolutions

www.pkisolutions.com

linkedin.com/in/thepkiguy

linkedin.com/company/pki-solutions