trust yourself.

P3KI Core

Technology Abstract

1 The State of Trust Architecture

Existing trust architectures suffer from several shortcomings.

X.509 breaks down if a root or intermediate certificate authority needs to be revoked[1], taking all client certificates in the field with it and requiring new certificates to be rolled out to each and every device. While X.509 offers some pre-defined levels of trust, these are at best rudimentary and unable to adequately address the wide range of possible scenarios. Also, changing the level of trust between two parties requires creation of new certificates, invalidating previously rolled out ones. Furthermore, X.509 dependence on central infrastructure for key distribution and especially handling of revocations easily becomes a liability in attack scenarios.

PGP gives you a piece of data you can use right of the bat, but to do so safely and securely a multi-step process is required to verify it. More often than not these steps are either forfeit entirely or replaced by out-of-band verification methods. Trust levels in PGP also tend to be mostly an annoyance. For automated systems, trust level checks are usually either disabled or all keys are trusted with ultimate level.

Ticket systems like Kerberos offer better modeling of trust levels and also support short-lived trust by design. However, they too rely on central infrastructure and setting them up is often described as painful and tedious.

2 P3KI Core - Combining the Good Parts

P3KI Core is a novel ***authorization and authentication solution*** based on resilient web-of-trust principles:

- ***Update trust*** to, as well as trust issued by, intermediaries ***easily*** and ***without invalidating*** trust of ***leaf nodes*** already in the field
- Express ***trust at arbitrary resolution and granularity***. You are in full control
- Model every trust scenario from ***strong hierarchies*** to ***heterogeneous mesh networks***
- Be ***independent of specific transports*** or storage media
- Run it centralized or ***distributed for increased resiliency***
- Verify trust even while ***fully offline***
- Integrate it easily into existing systems, either as a ***micro-architecture service*** or native ***library***[2]

Therefore, P3KI Core offers increased ***resiliency***, actual ***graceful degradation***, and far higher ***flexibility*** at ***lower operating costs*** when compared to existing solutions.

P3KI Core is trust you can understand.

[1] See the Diginotar and TurkTrust debacles in 2011 and 2013 respectively as well as Symantec issuing a rogue Extended Validation certificate for google.com in 2015.

[2] Library written in Rust offering C-ABI targeting common platforms like x86_64, ARM, Apple iOS, and Google Android

3 Trust Relationships: Communication & Storage

P3KI Core does not rely on any specific storage or communication backend. Nor do parties who published their trust relationships need to be online for others to access their information.

Relationships can be stored in a central database, a distributed peer-to-peer network, or even communicated offline via sneakernet-like[3], opportunistic approaches. P3KI Core does not require any security guarantees from its storage and communication backend.

All trust data is cryptographically signed to ensure verifiability at all times. Being able to do online checks for updated trust data offers additional benefits; however, trust data can be verified fully even in offline scenarios.

4 Take Back Control

Existing solutions work because a set of trust anchors – root certificate authorities – which are deployed to each and every device (e.g. mobile phone, webbrowser, operating system) decide for you who it is you'll trust.

With P3KI Core you yourself and each of your devices are their own trust anchor. You decide who to trust. You have full control.

5 Expressing Trust

Trust can be expressed in arbitrary granularity. You do not have to rely on pre-defined trust levels when modeling your scenario.

Trust between parties is expressed using trust policy languages tailored to your specific scenario, yet still offering flexibility to be future compatible, accommodating shifting requirements.

You can be as specific and detail oriented as you want in expressing trust. Even better: you can introduce new or finer trust levels after your system has been rolled out without having to update existing devices!

6 Delegation: A first-class Citizen

Delegation of trust is a first-class feature of P3KI Core. This finally makes the sharing of keys – which happens normally within existing systems – legible and quantifiable.

Trust policy Languages are based on mathematical principles which are provable and ensure a single, well-defined interpretation across all participants. If Alice trusts Bob and Bob trusts Claire, P3KI Core can decide based on Alice's and Bob's trust relationships whether and if so exactly how much Alice can trust Claire. This does not require Alice to directly trust Claire nor does it require Alice to have heard about Claire ever before.

This is true delegation.

[3] Informal term describing the transfer of electronic information by physically moving media from one computer to another.

7 React to Compromise without Compromising your Operation

Trust changes over time. Either by evolution or by force.

Changing your mind is very inexpensive with P3KI Core. It supports real, short-lived trust akin to ticket systems. Publishing updated trust relationships entails the calculation of a few hashes and a single cryptographic signature operation.

Common trust networks – usually built on multiple certificate authorities (root and intermediates) – have multiple critical flaws once an intermediate gets compromised[4].

Most obvious is the need to revoke the compromised intermediary. Most costly is the need to re-issue and re-distribute new certificates to everyone having used certificates signed by the intermediary. Most overlooked is the need to communicate a revoked certificate which usually requires central infrastructure (like a CRL[5] or OCSP[6] server) which is an easy target not just for state actor players.

P3KI Core allows smooth transitions away from compromised intermediaries without the need to re-issue certificates for leaf nodes.

P3KI Core can be operated without any central infrastructure making it very resilient to even organized attack. It can even be operated over opportunistic sneakernet-like offline networks, thus offering zero attack footprint.

P3KI Core offers the ability to implement graceful degradation for your authorization and authentication network.

8 P3KI GmbH

Operating since 2014 with a top-notch, international team we're building the next generation of PKI and trust architectures. P3KI Core technology is based on more than eight years of research, multiple best-of-class thesis works and years of experience in the IT security and software development world. P3KI GmbH is a privately owned subsidiary of berlin-based IT security consultancy Recurity Labs GmbH.

[4] See the Diginotar and TurkTrust debacles in 2011 and 2013 respectively as well as Symantec issuing a rogue Extended Validation certificate for google.com in 2015.

[5] Certificate Revocation List. A list of digital certificates that have been revoked by the issuing Certificate Authority.

[6] Online Certificate Status Protocol. Used for obtaining the revocation status of an X.509 digital certificate.