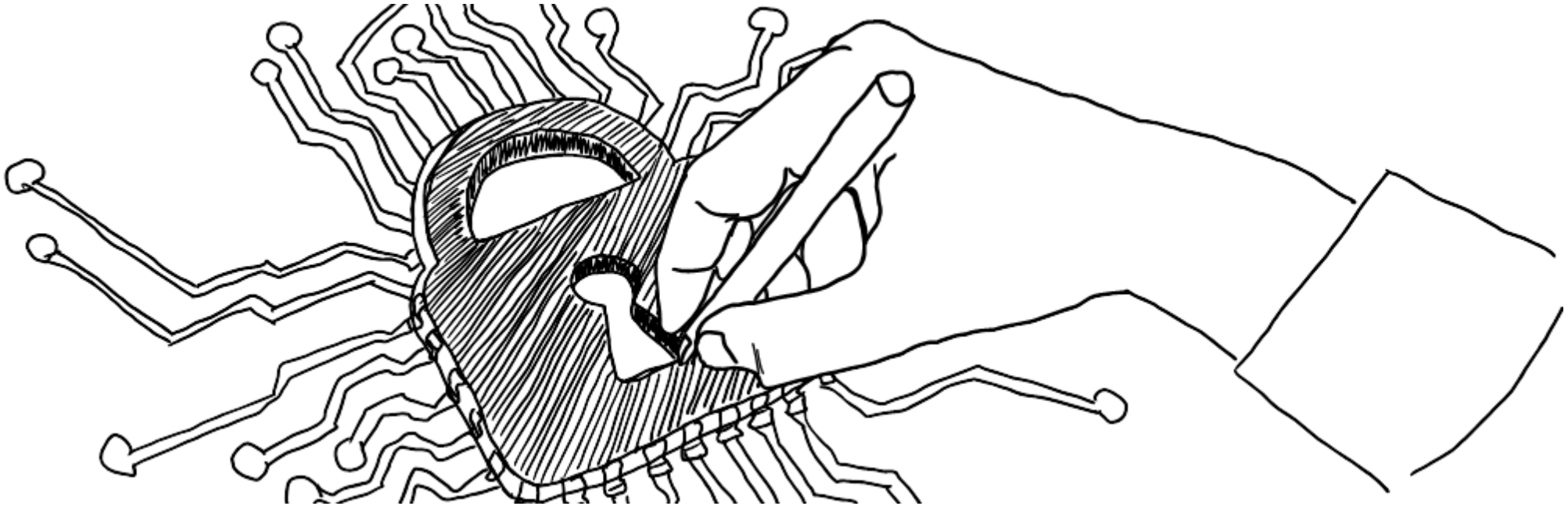
zühlke
empowering ideas



IoT – user needs vs. security

PKI to the rescue!

 © Zühlke 2019

1. User experience first
2. Challenges of the IoT
3. PKI to the rescue?
4. PKI to the rescue!

User experience first

UX is not visual design

UX is …

- User eXperience design
- User interaction design
- Human computer interaction
- Workflows
- … it doesn't necessarily have to look good!

UX is not visual design

UX Designers do …

- Requirements, user stories
- User interviews, user observation
- Define personae
- Interaction design prototyping
- Usability testing

Good UX is sometimes in conflict with good security?

Warning

If you don’t enter the correct password within the next 5 attempts, your phone will automatically be reset to factory settings and all information on the phone will be erased.

Convenience

~~Good UX~~ is sometimes in conflict with good security!

- Find good compromises
- UX designers are allies

 © Zühlke 2019

Don’t try to build un-hackable systems!

Instead, build systems that

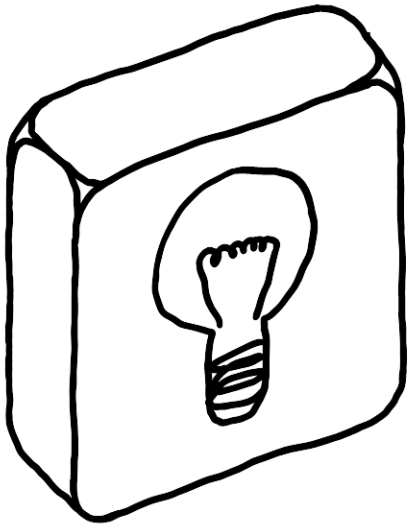
- Don’t put your users at risk
- Offer good compromises between convenience and security

It’s frequently not an option to deny service because of the failure of a security system.

 © Zühlke 2019

Challenges of the IoT

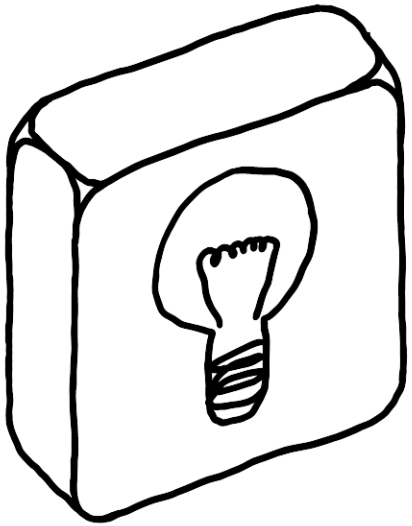
Device identity



- Device serial number
- Hardware addresses
- Installation location
- Linked customer account
- Local network addresses

 © Zühlke 2019

Device provisioning

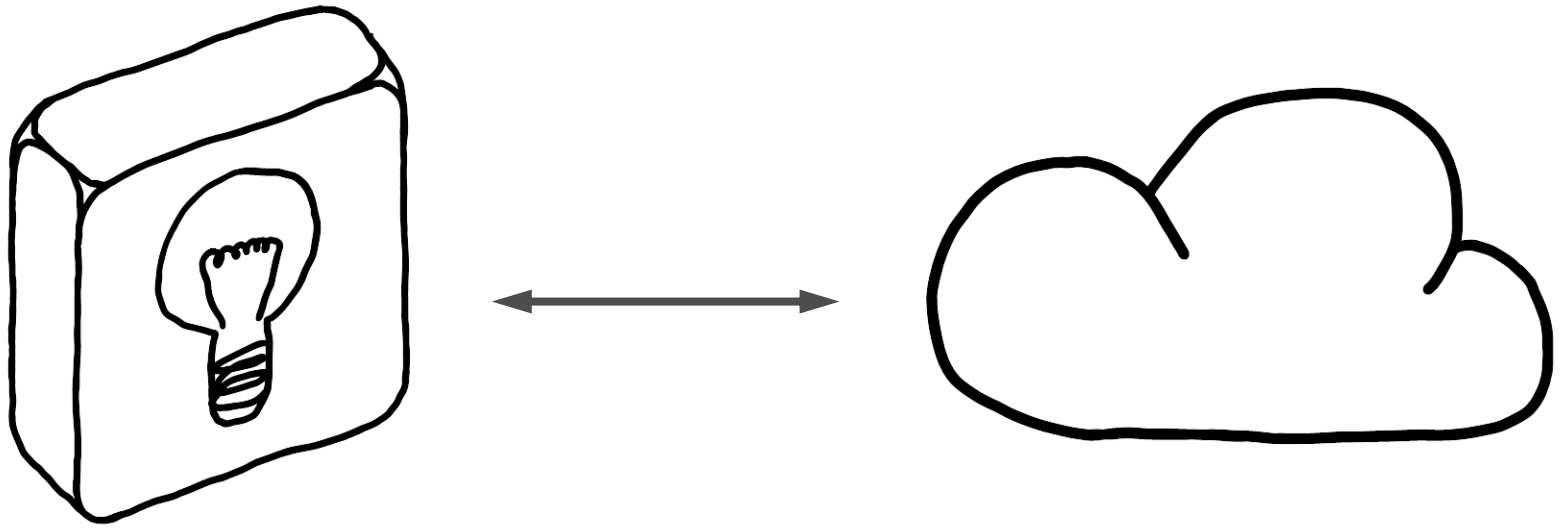


Provisioning process

- Mainly at installation time
- Merge device identities
- Supply configuration
- Supply cryptographic keys

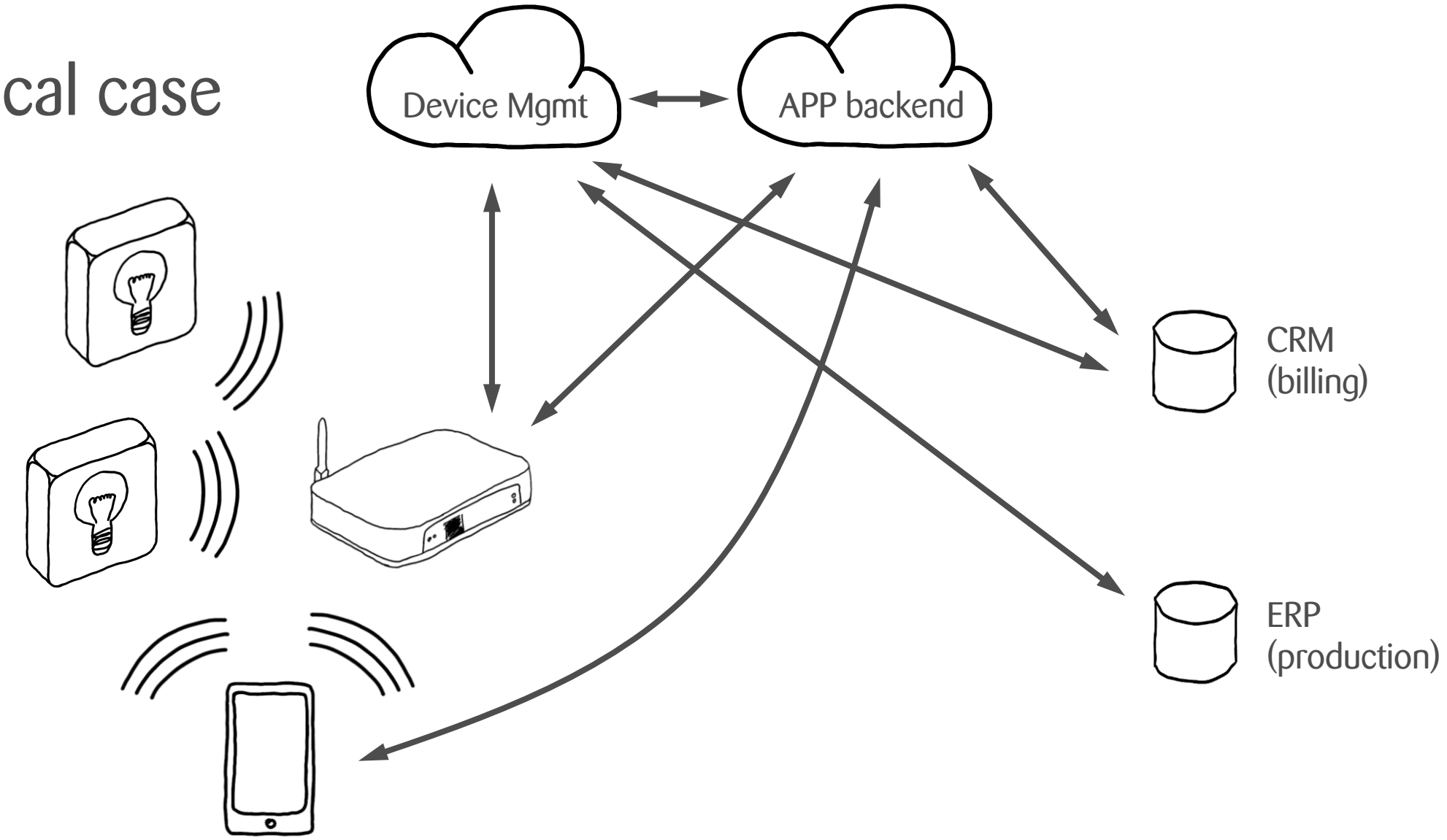
 © Zühlke 2019

Simple case



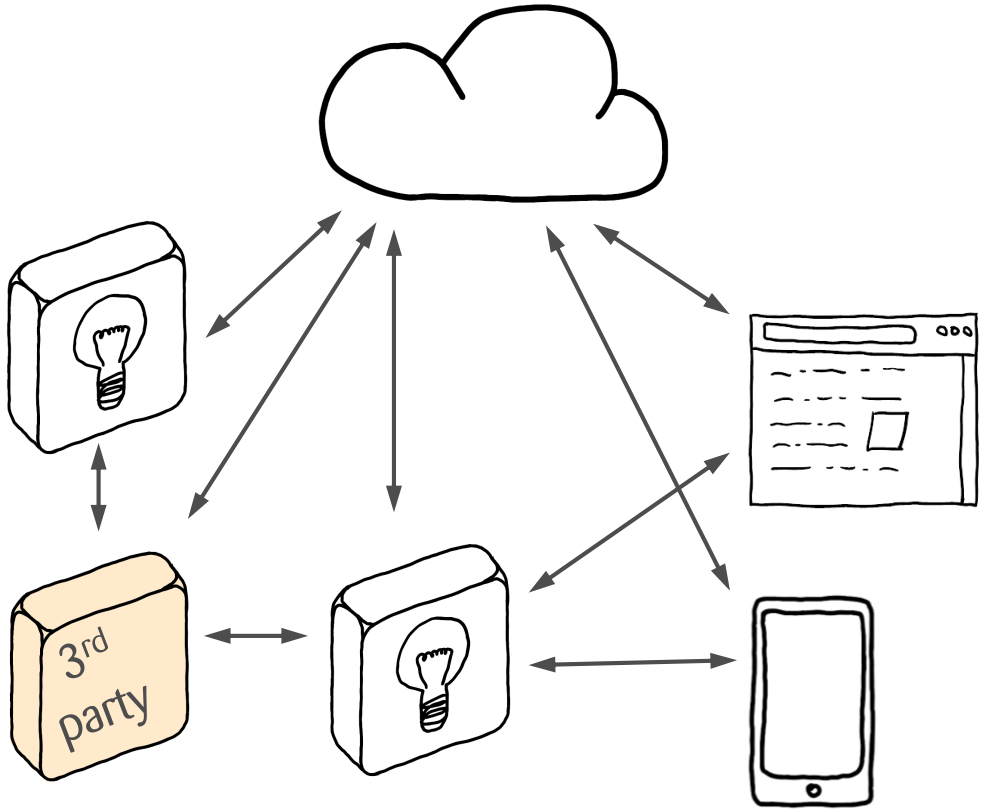
 © Zühlke 2019

Typical case

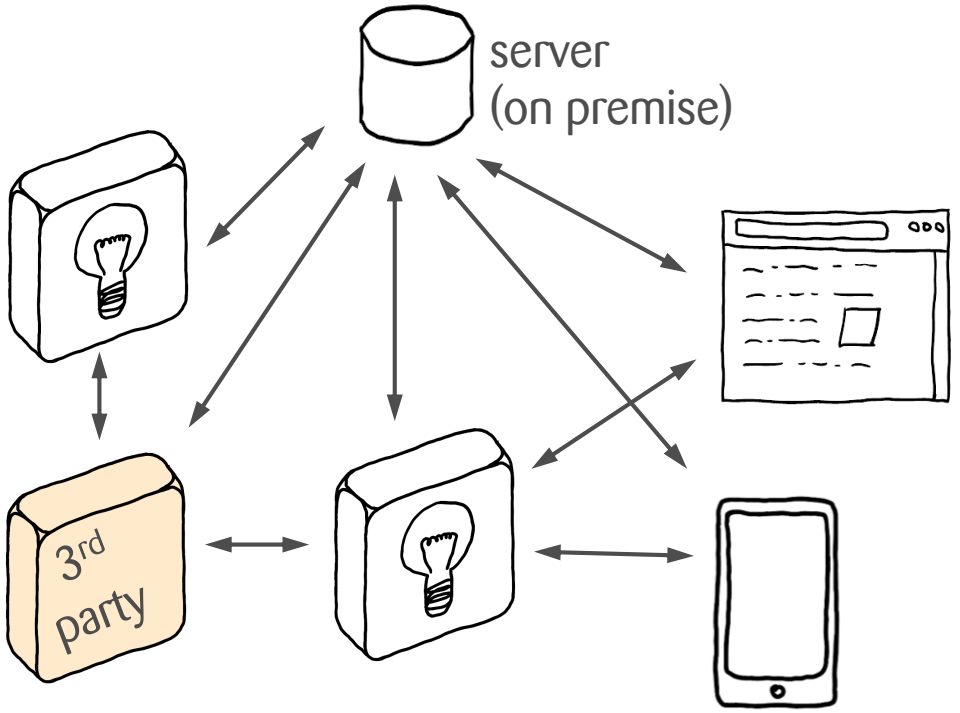


 © Zühlke 2019

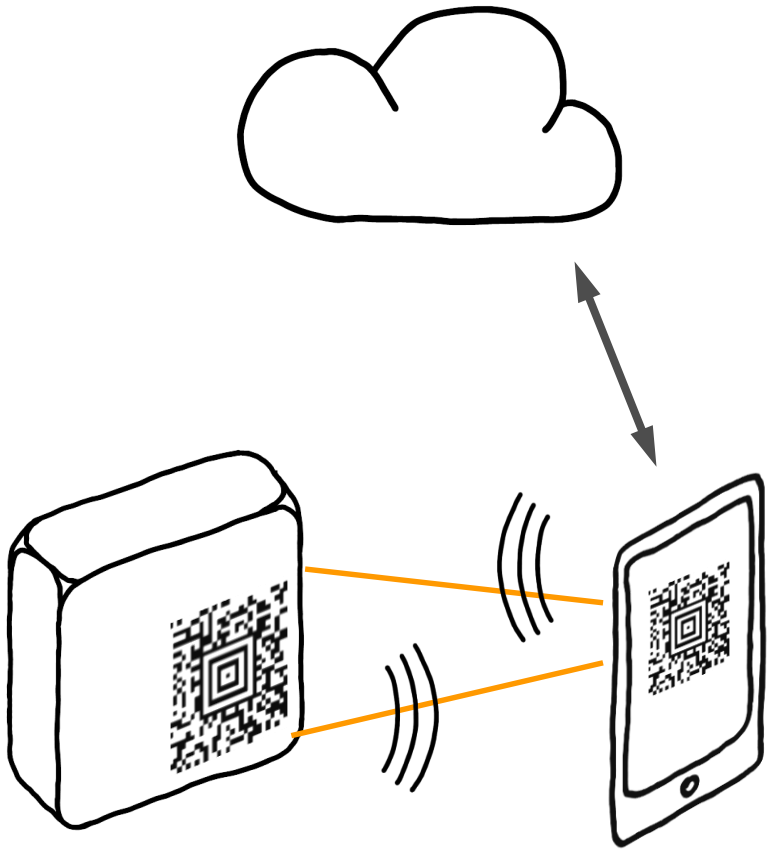
Complicated cases



Offline Case



Secure provisioning



 © Zühlke 2019

PKI to the rescue?

 © Zühlke 2019

Nobody understands certificates

A X509 certificate is a document that links an _____ to a ____ _____.

It is _____ by a certification authority.

 © Zühlke 2019

Nobody understands certificates

A X509 certificate is a document that links an `identity` to a `key pair`.

It is `signed` by a certification authority.

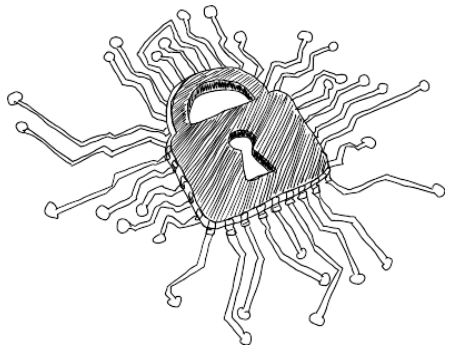
X509 certificate

Identity

- some.dns.name
- 
- 01:02:03:04:05:06

Key pair

- RSA
- ECC

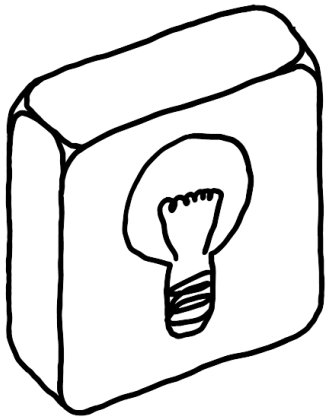


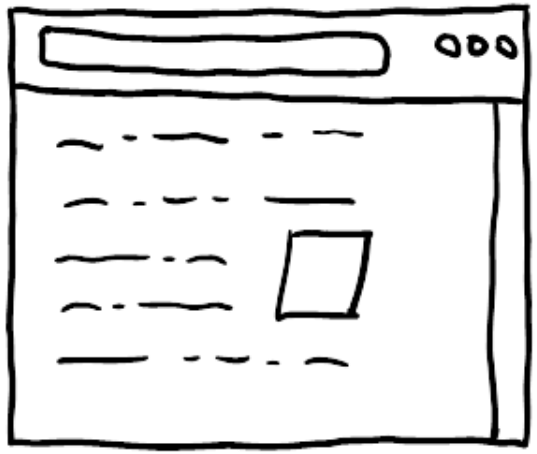
Signature by
trusted third party

 © Zühlke 2019

Browsers vs. IoT

- Device serial number
- Hardware addresses
- Installation location
- Linked customer account
- Local network addresses / URL





 © Zühlke 2019

Antipattern: Enable TLS at all cost

- Goal: Enable TLS on some device
- TLS needs certificates
- We don’t know the identity beforehand (IP-addr, hostname)

→ Simply deploy CA with the device!

 © Zühlke 2019

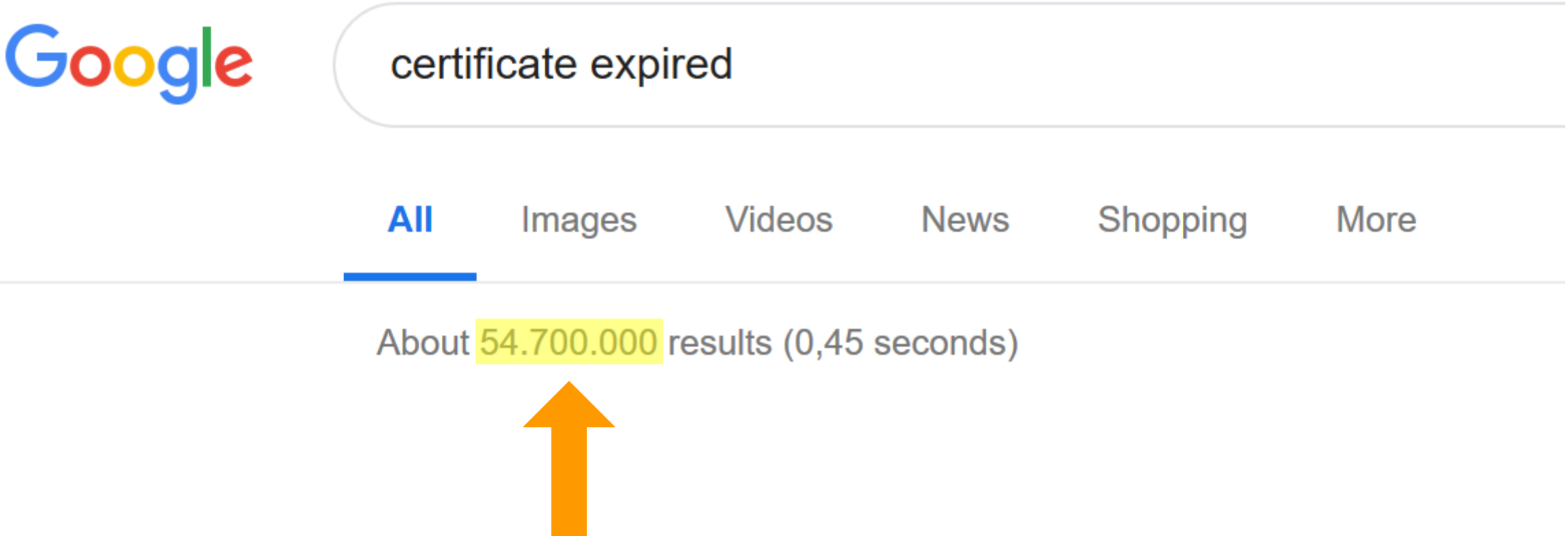
100% of PKI failures are not because of an attacker[1,2]

People react rationally:

- Press random stuff until the error goes away
- Yell at the contractor
- Vent their frustration on Twitter

[1] Ok, it's probably 99,9999%
[2] Alternative explanation: PKI is so successful that nobody tries to attack

 © Zühlke 2019


Google
certificate expired
All
Images
Videos
News
Shopping
More
About 54.700.000 results (0,45 seconds)

 © Zühlke 2019

Why do certificates expire after two years?

Argument: To limit exposure in case of compromise.

→ But two years is no more acceptable than twenty years!

→ The argument is invalid unless we limit exposure to something acceptable, e.g. 6 hours.

→ Use revocation to limit exposure!

 © Zühlke 2019

Why do certificates expire after two years?

Argument: To force deprecation of unsafe crypto standards.

→ Yes, but configuration can do that as well.

Why is the link between identity and key pair valid until the expiration date, and then invalid one second later?

To protect the business model of the certification authority?

 © Zühlke 2019

What does the user want?

 © Zühlke 2019

In an IoT context, certificates that expire are like Y2K on purpose!

 © Zühlke 2019

Unique selling point of PKI

Enable two unfamiliar parties to:

- Authenticate each other
- Establish an encrypted channel

Mostly Offline (without active participation of trusted third party)

Except that it doesn't work because revocation doesn't work offline.

 © Zühlke 2019

PKI Alternatives

- Pre shared keys
- Kerberos
- SSH
- TLS/RPK (raw private key)
- TLS/PSK (pre shared key)
- Non-X509 certificates
- Biometrics
- Secure elements, smart cards
- Block chain
- PUFs (physically unclonable functions)

 © Zühlke 2019

PKI to the rescue!

Is PKI a good compromise?

- Web scenario
- Enterprise scenario
- Mobile scenario
- IoT scenario

 © Zühlke 2019

Many UX challenges for cyber security happen because things were designed to reflect technical correctness – but didn't necessarily align with user interpretation.

 © Zühlke 2019

PKI in IoT-Scenario

UX-Advice:

Never ever show a certificate to an end-user!

Use metaphors:

Security token, passport, …

PKI in IoT-Scenario

UX-Advice:

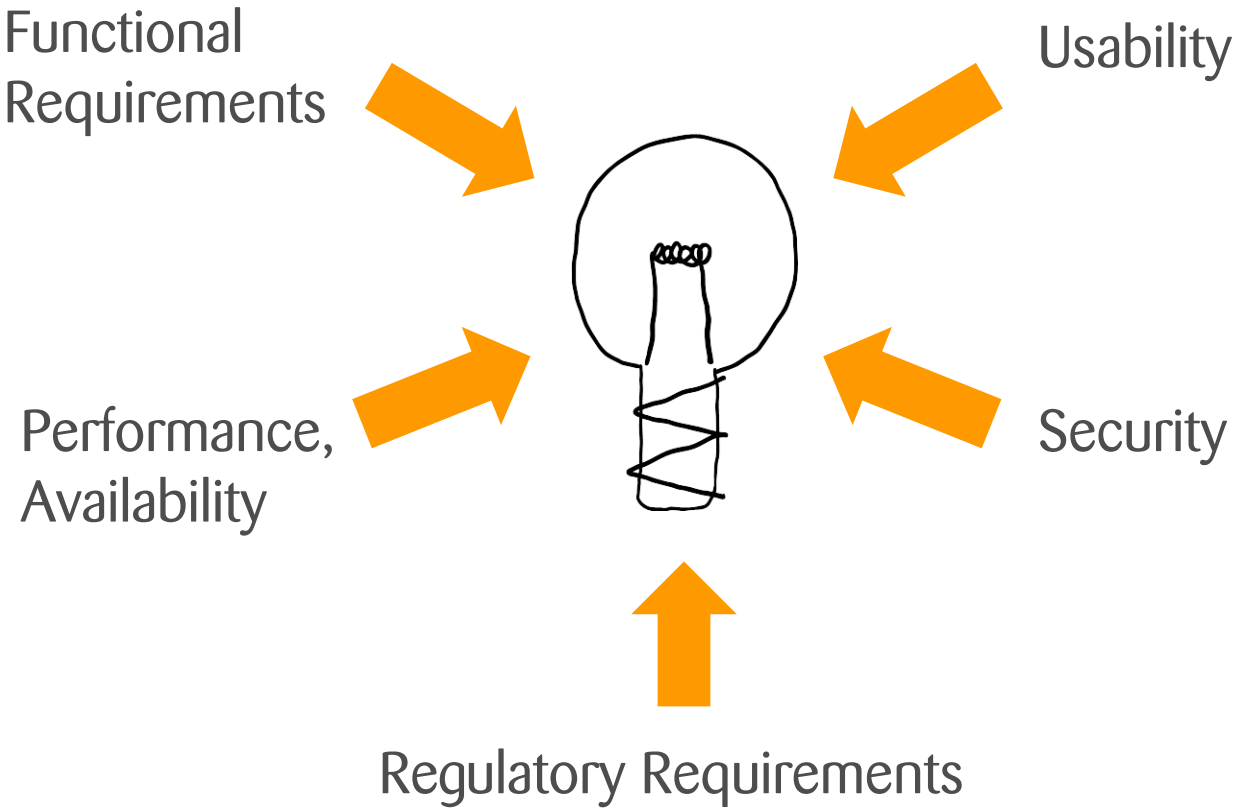
Don’t use hard expiry dates for certificates.

Use “best before” dates.

If expiry is necessary, make renewal automatic and transparent.

 © Zühlke 2019

So, what makes a product great?



 © Zühlke 2019

Security with bad UX is bad security!

 © Zühlke 2019