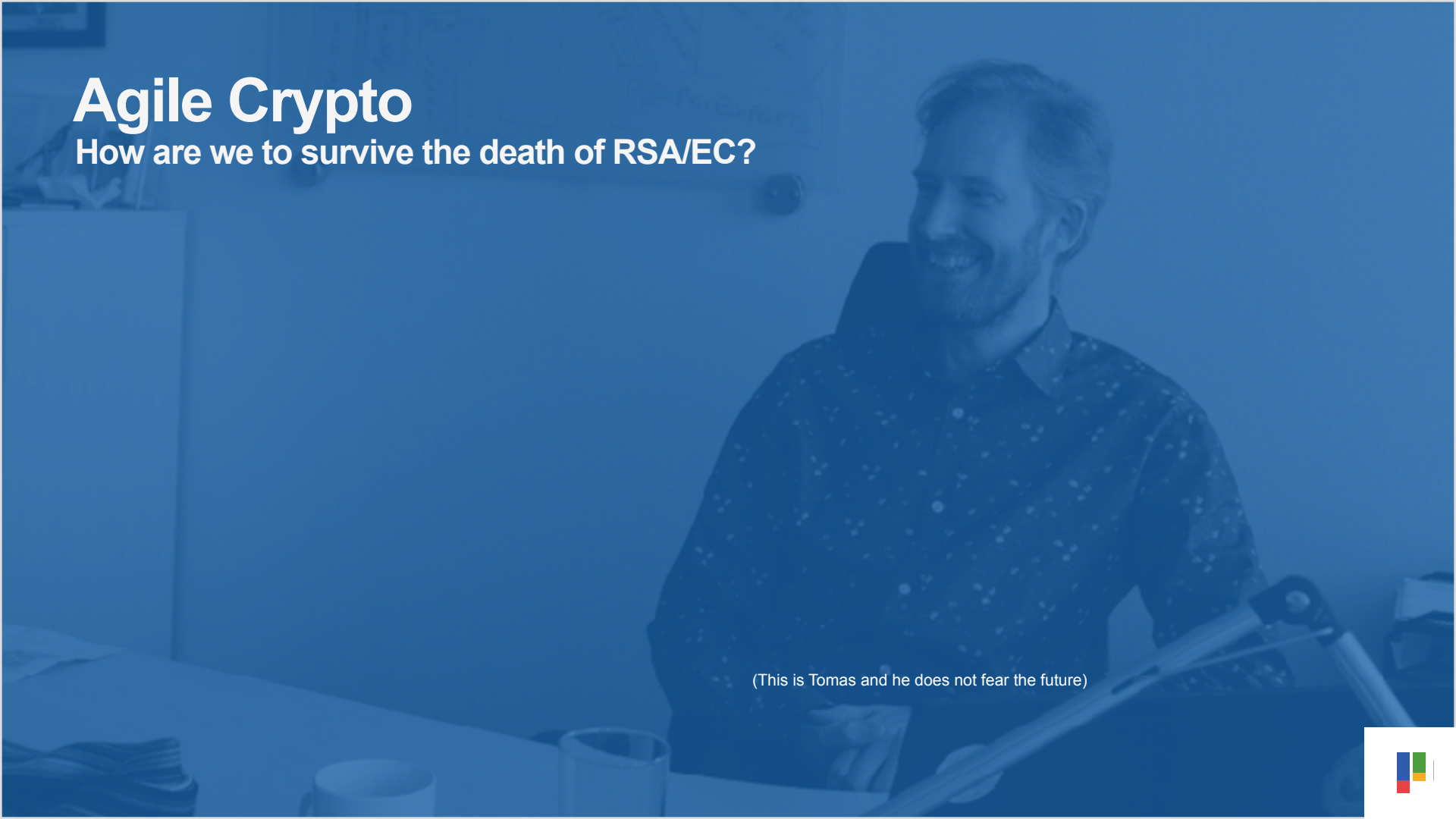

PrimeKey

# Agile Crypto

## How are we to survive the death of RSA/EC?



(This is Tomas and he does not fear the future)

# Agenda

- About PrimeKey Solutions
- Who I am and why PrimeKey are here
- Why Agile PKI as a Topic?
- Post Quantum Crypto - A Timeline
- Current Solutions and their Feasibility
- Where do we go from here?

**Interrupt at any time.**



# About PrimeKey Solutions

- Working in Open Source PKI Since 2001
- Develop and maintain three PKI software projects:
  - EJBCA
  - Signserver
  - NPKD
- Develop the hardware platforms PKI Appliance and SEE
- ~70 employees in three countries

**Selected Customers and Partners**

dun & bradstreet, worldline, AIRFRANCE, dimension data, SIEMENS, digicert, GlobalSign, QuoVadis, ZENDITS, SGS, ITCARD, bankgirot

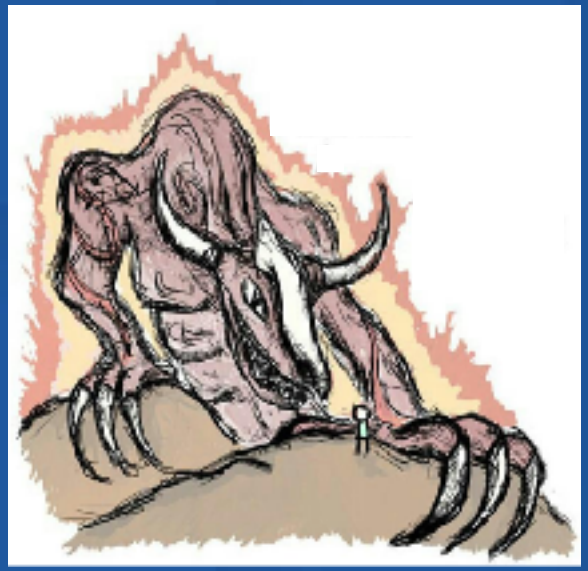
**Offices**

Stockholm, Sweden
Head office

Aachen, Germany
Hardware development

Silicon Valley, USA
Sales and consulting

# Who I am and why PrimeKey are here



"You should not have come here, feeble developer. Why do you attend CABForum?"

"I figured I was going to talk Agile PKI."

"You expect to hold a workshop and leave here alive, knowing that Ryan Sleevi is in the audience?"

"I am not a clever man"

# Who I am and why PrimeKey are here

- Mike Agrenius Kushner
- Product Owner EJBCA
- Been in PKI for ~8 years
- Probably not the smartest person in this room.



# Who I am and why PrimeKey are here

As a PKI vendor, PrimeKey's goal at CABForum is to

- stay at the forefront of developments in the PKI ecosystem
- bring to the table 20 years of experience in certificate issuance and signing operations
- be able to weigh in on implementation details and timelines from a vendor's POV



# SCEP

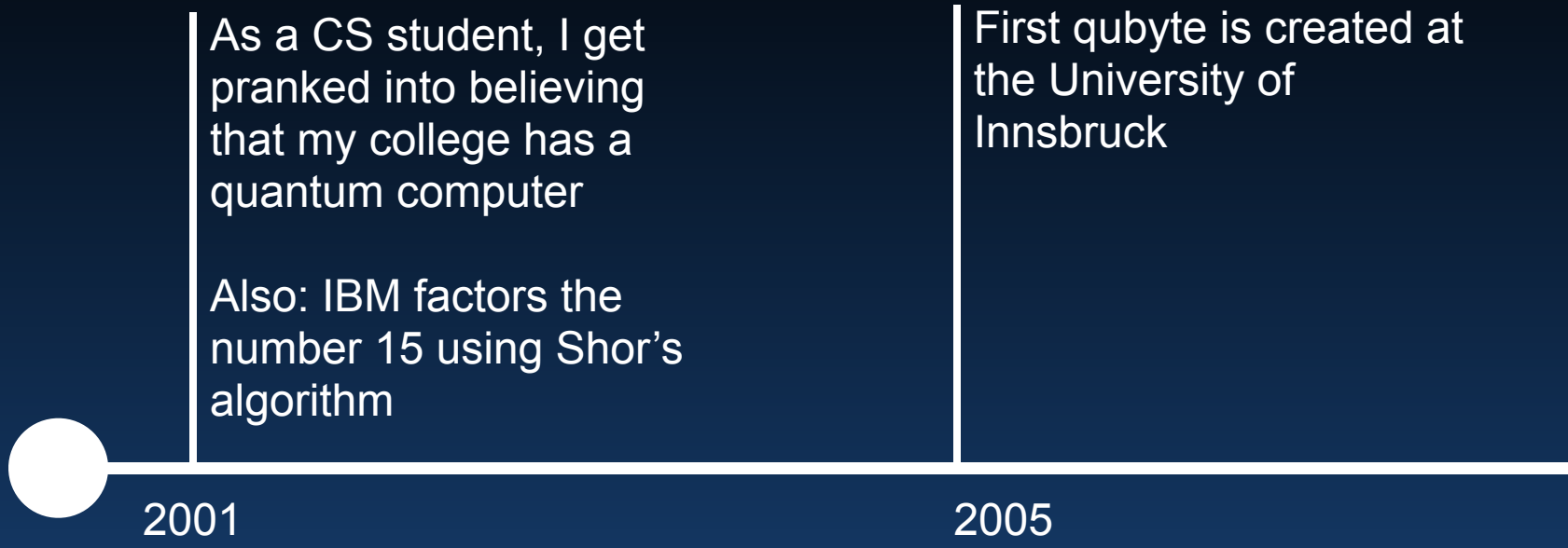


# Why Agile PKI as a topic?

- Great way of getting a speaking slot in 2018
- Everybody is talking algorithms - no point unless there’s agility
- There are plenty of non-scifi usecases
- We want to hear your views and opinions.

# Post Quantum Crypto

A brief and incomplete timeline



2009

NIST reads, writes qubits, demonstrates multiple computational operations

2012

Chinese researchers believe they have factored 143 using Shor's algorithm.

2014

Researchers show that the previous group actually factored 56153 without being aware of it (though not as a general algorithm).

Snowden files show that the NSA have an active interest in QC.

2016

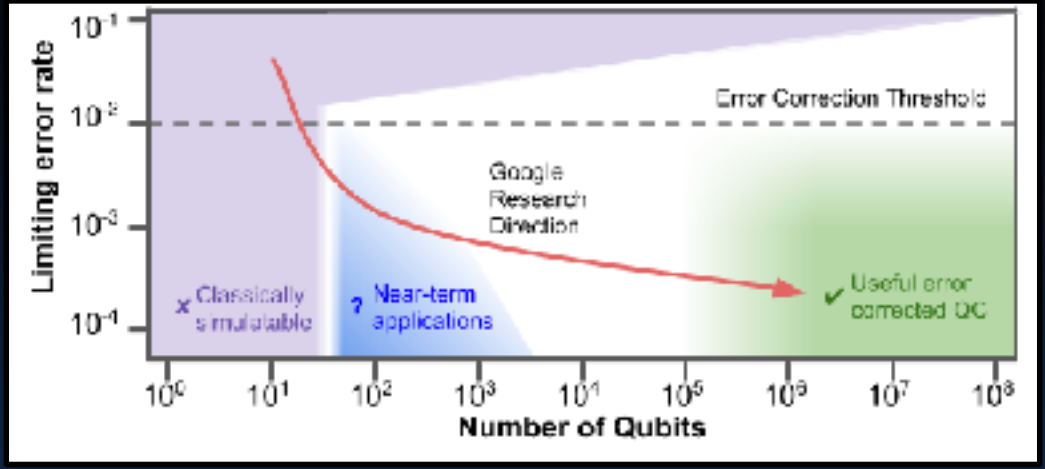
Google experiments with a PQ algorithm in Chrome Canary.

2017

IBM unveil a 50 qubit quantum computer

2018

Google develops Bristlecone, a 72 qubit quantum processor

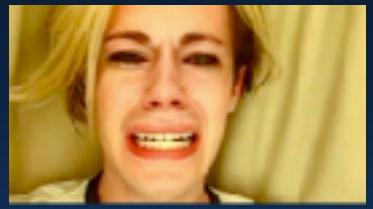



*(Source: Google Quantum AI Lab)*

Doomsday Equation according to ETSI EG 203 310 [i.4]:

- X = the number of years the public-key cryptography needs to remain unbroken.
- **Y = the number of years it will take to replace the current system with one that is quantum-safe.**
- Z = the number of years it will take to break the current tools, using quantum computers or other means.
- T = the number of years it will take to develop trust in quantum-safe algorithms.

If X + Y + T > Z then



My Translation:

- X = the longest validity of a certificate issued today in a PKI
- Y = the number of years it takes to establish an Agile PKI standard and implement that standard universally
- Z = the number of years until a quantum computer can solve factorization/discrete logarithm problems + computation time
- T = the number of years it will take for a PQ algorithm to be adopted

# Post Quantum PKI

## Why I’m Wasting your Time on this Matter

- Crypto Agility has other uses than just post-quantum, i.e. preparing the ecosystem to be able to handle a massive and sudden rekeying process
- The infrastructure needed for a catastrophic rekeying needs to be in place in good time beforehand.
- CA/Browser Forum are far from the only stakeholder, but one of the most nimble. Where you lead, others may follow.
- Open standards = Healthy Ecosystem



# Post Quantum PKI

Our Own Contributions so far

- Had an intern evaluate and benchmark X509 Certificates signed with post quantum algorithms as his thesis (https://www.primekey.com/wp-content/uploads/2017/08/post-quantum-algorithms-for-pki.pdf)
- We are currently researching the field of Agile Cryptography in PKI, talking to experts and HSM vendors



# Current (known) Solutions and their Feasibility

On the day of Ragnarök:

1. all issued certificates for our customer PKI's must be able to safely and instantly migrate to post-quantum certificates
2. all issued keys (for PKIs using client side authentication) must have a migration strategy to equivalent post-quantum key pairs

# Current (known) Solutions and their Feasibility

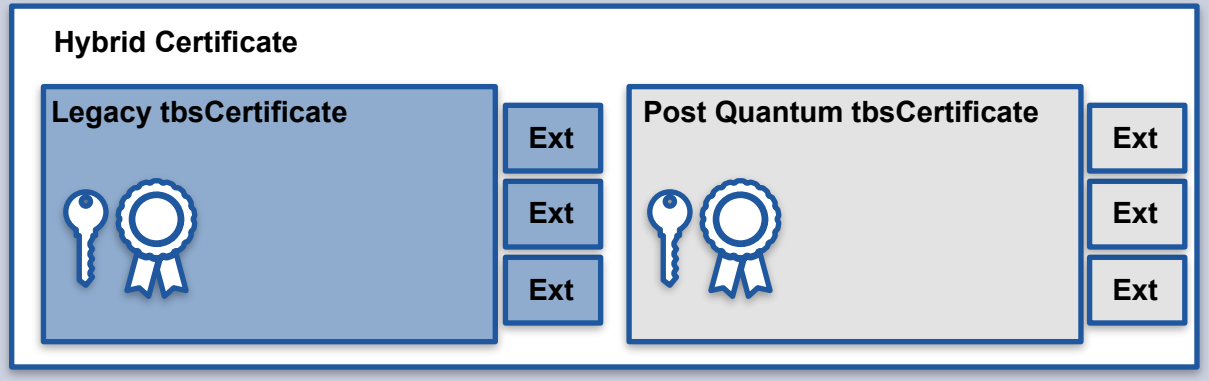
Known strategies:

- Hybrid Certificates
- Post Quantum Certificate Extensions



# Current (known) Solutions and their Feasibility

| Strategy | Hybrid Certificates |
| --- | --- |



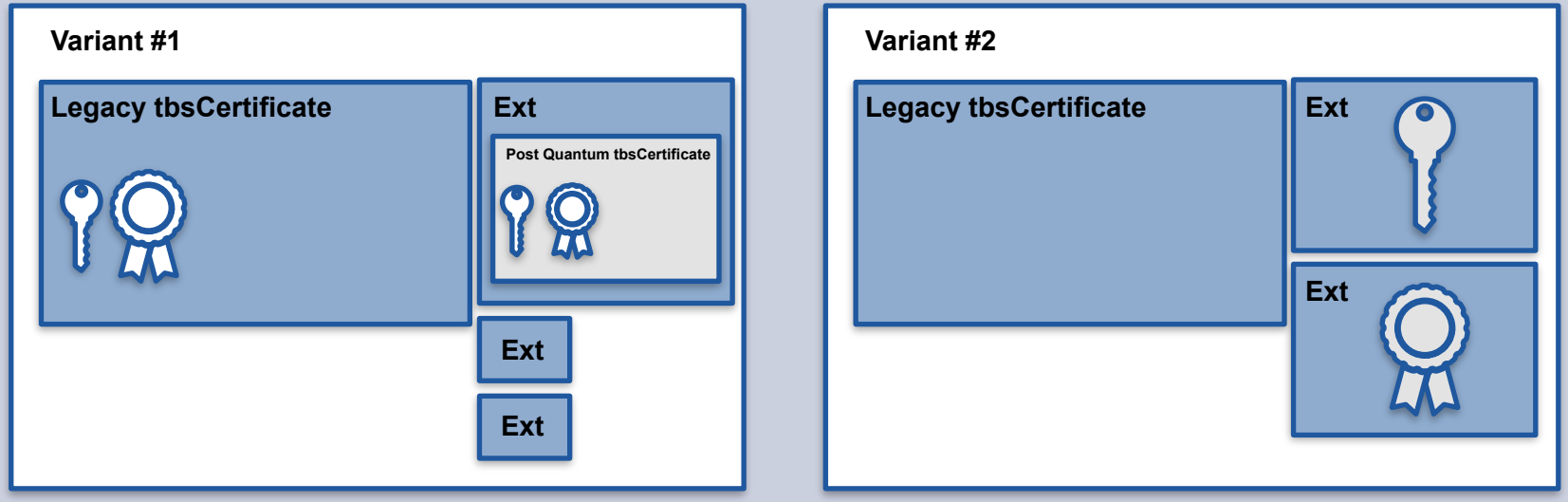
# Current (known) Solutions and their Feasibility

| Strategy | Hybrid Certificates |
| --- | --- |
| Pros | • Conceptually simple |
| Cons | • Requires rewriting RFC5280<br>• Not backwards compatible (can/should a tbsCertificate body be non-critical?)<br>• May create huge certificates (~5MB) with no gain if QC never becomes a reality |



# Current (known) Solutions and their Feasibility

| Strategy | Post Quantum Certificate Extension |
| --- | --- |




*[1]: https://tools.ietf.org/html/draft-truskovsky-lamps-pq-hybrid-x509-00*

# Current (known) Solutions and their Feasibility

| Strategy | Post Quantum Certificate Extension |
|---|---|
| Description | Adding additional fields and (non-critical) extensions to X509 Certificate containing either a PQ tbsCertificate-body, or a merely public key and signature references |
| Pros | • There is already a draft submitted by Cisco, Entrust and ISARA[1]<br>• Could potentially allow for multiple PQ signatures<br>• Backwards compatible |
| Cons | • May also inflate certificate sizes |

*[1]: https://tools.ietf.org/html/draft-truskovsky-lamps-pq-hybrid-x509-00*

# Where do we go from here?

Open Questions:

- When would you like to see PQ Root CAs available?
- Would anybody want to perform interoperability tests on currently implemented PQ algorithms in BouncyCastle (Rainbow, SPHINCS)?
- What would you like us to do?

# Thank you for your time

mike.kushner@primekey.com

ReadMe: blog.ejbca.org