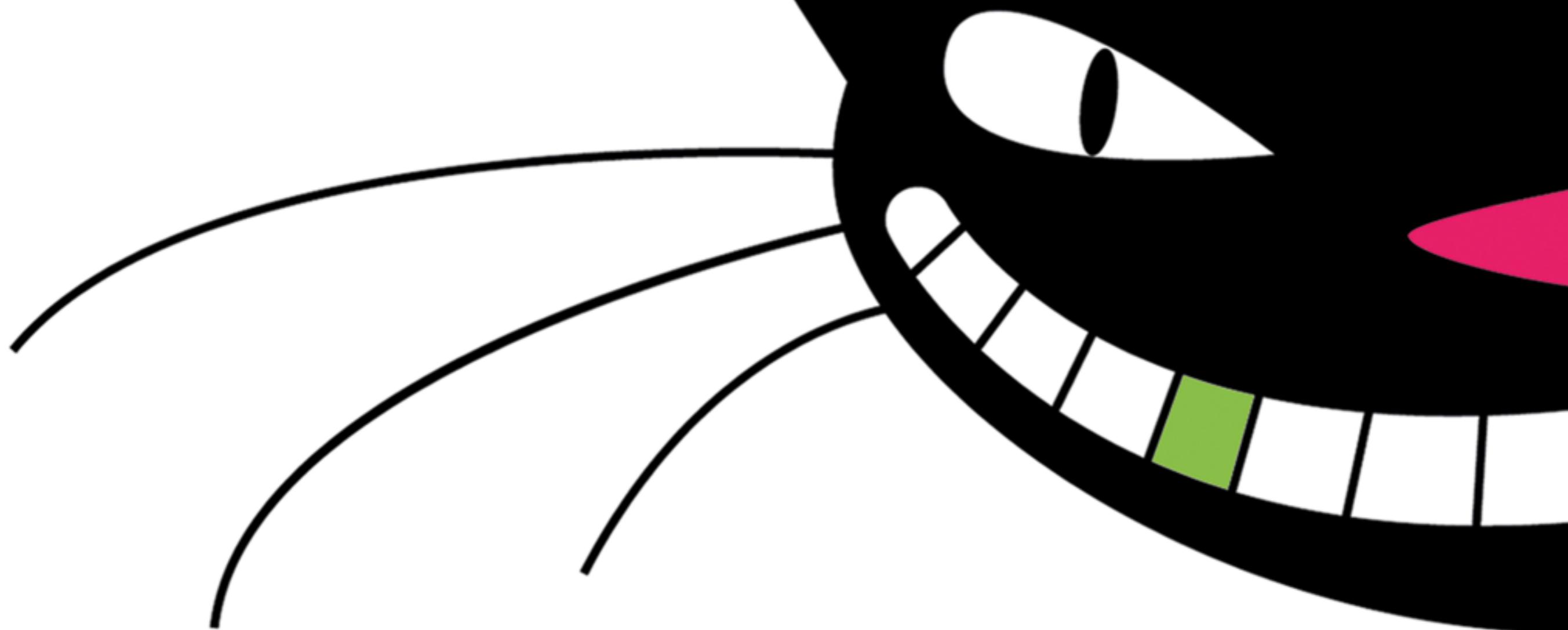


kinko.me



PRETTY EASY PRIVACY

05-2014

It is called kinko

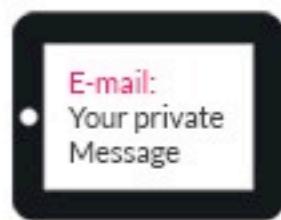
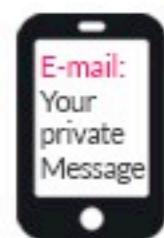
Easy E-mail encryption to protect your privacy:



↔
the internet



↔
secure connection



pretty easy privacy: activated

Overview

- ▶ introduction
- ▶ spot the problem
- ▶ building good crypto tools
- ▶ challenges
- ▶ more than tools
- ▶ get involved

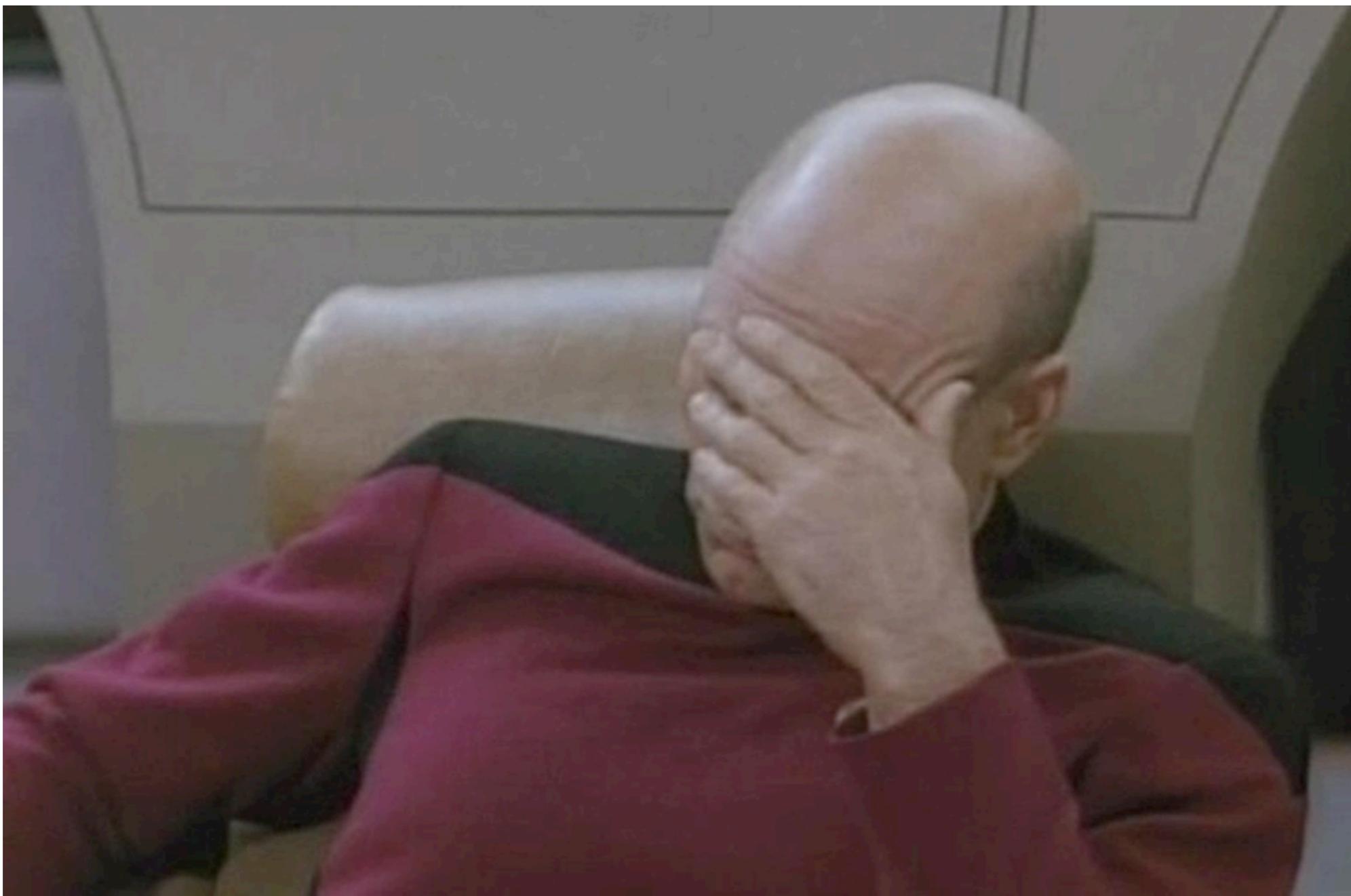
Snowden 2013...

...rekindled interest in privacy.

Privacy after 2013 means:

- ▶ **a pretty secure means of communication**
- ▶ **user interfaces that are accessible to everyone**

Spot the Problem



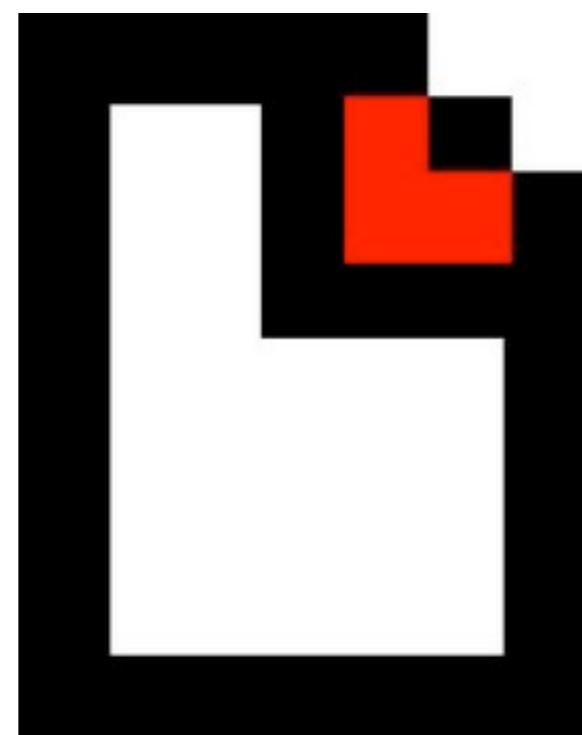
DE-Mail



DE-Mail



Lavabit



Lavabit

Lavabit



Posteo



CryptoCat



Threema, Apple iMessage



Thunderbird/Enigmail



Heartbleed





What has kinko learned

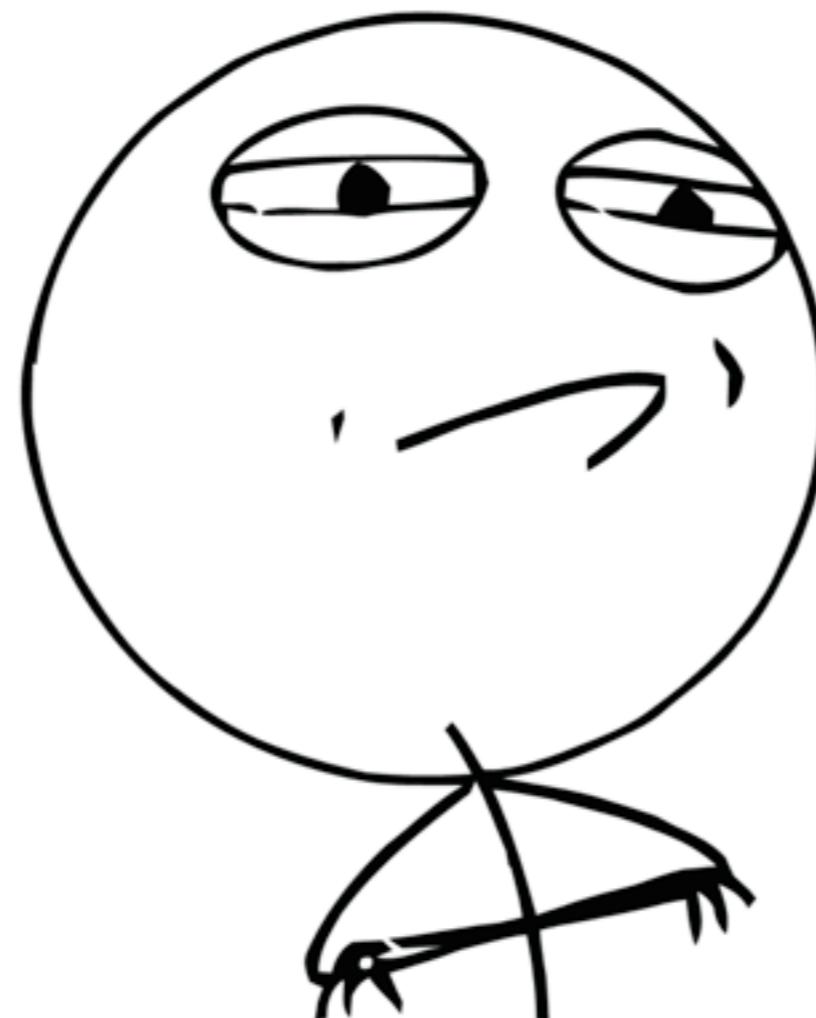
- ▶ easy-to-use
- ▶ OpenSource
- ▶ end-to-end encryption
- ▶ vibrant community
- ▶ do not make cryptography yourself
- ▶ consider browser and desktop security challenges

	kinko	DE-Mail	LavaBit	CryptoCat	Threema	Thunderbird/ Enigmail	OpenSSL
easy-to-use	✓	X	✓	✓	✓	X	✓
OpenSource	✓	X	X	✓	X	✓	✓
end-to-end encrypted	✓	X	✓	✓	✓	✓	✓
vibrant community	✓	X	X	✓	X	✓	X
know your cryptography	✓	X	✓	X	?	✓	✓
consider browser and desktop security challenges	✓	X	X	X	X	X	-
no need to trust the operator	✓	X	X	✓	X	✓	✓

Challenges

- ▶ Usability
- ▶ Mobility
- ▶ Desktop OS
- ▶ Identity
- ▶ Trust
- ▶ Security
- ▶ Community
- ▶ Fun
- ▶ Reaching Out
- ▶ Funding

CHALLENGE ACCEPTED

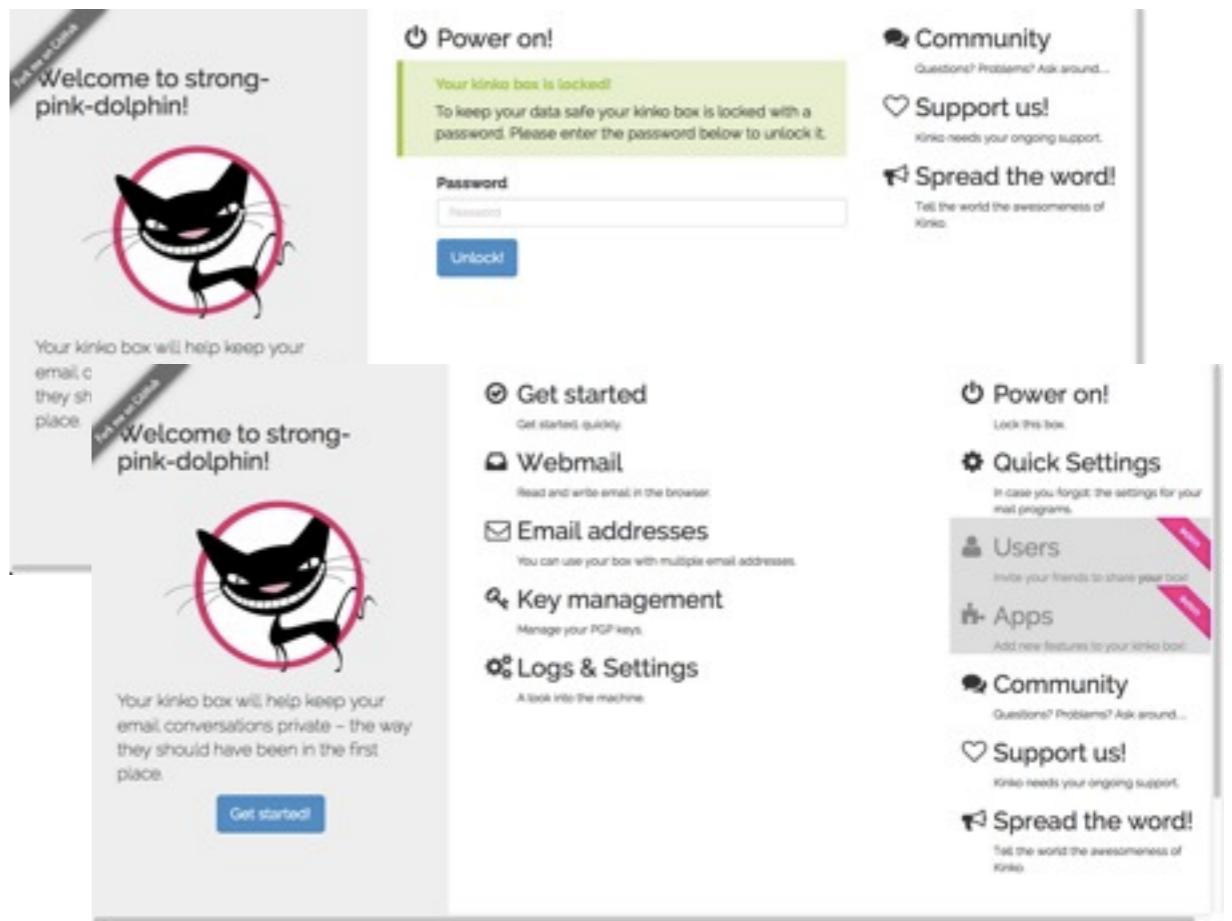


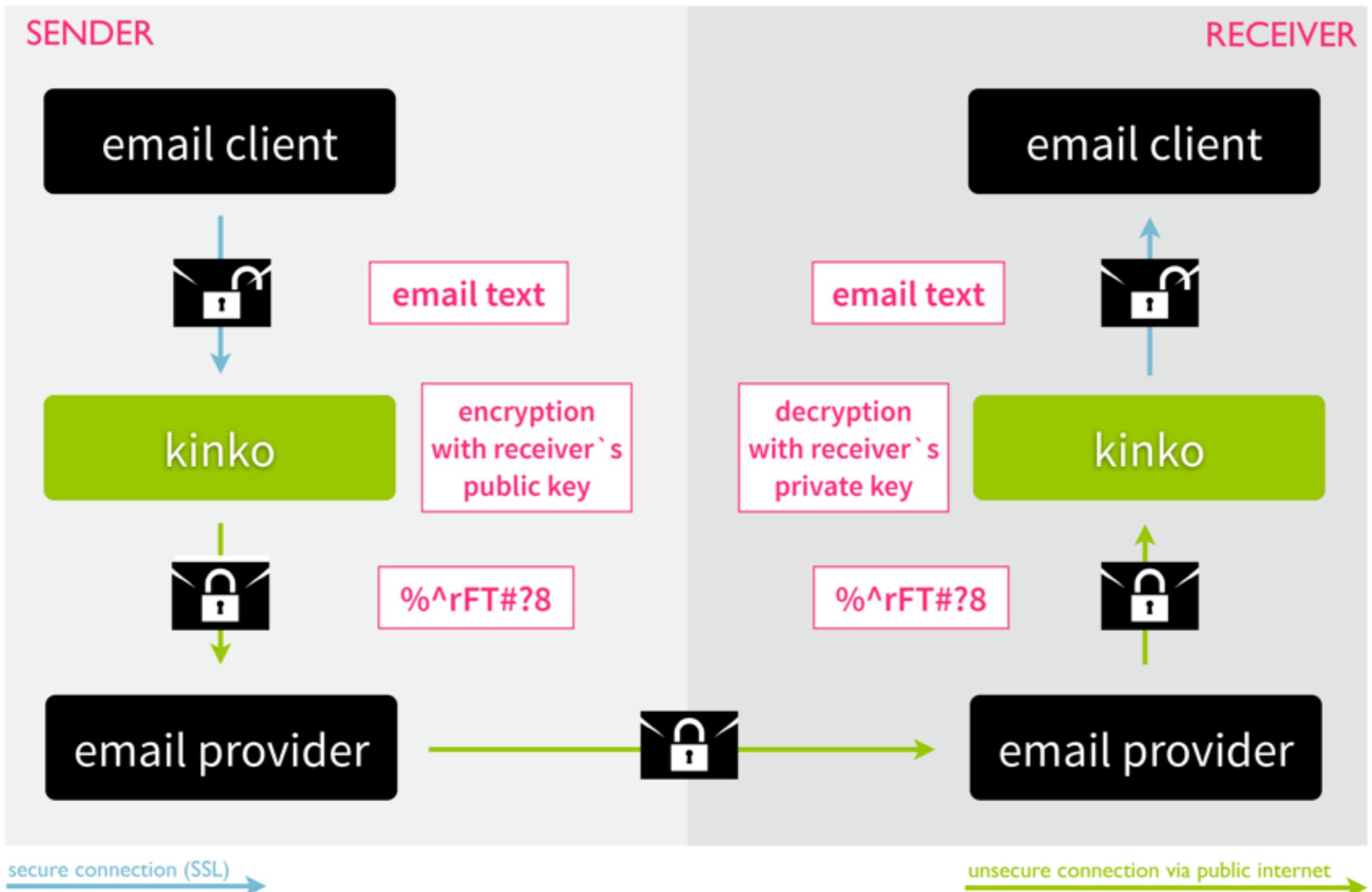
Challenge: Usability

- ▶ Usability determines mainstream adoption
- ▶ PGP exists for > 20 years: how many people are using it?

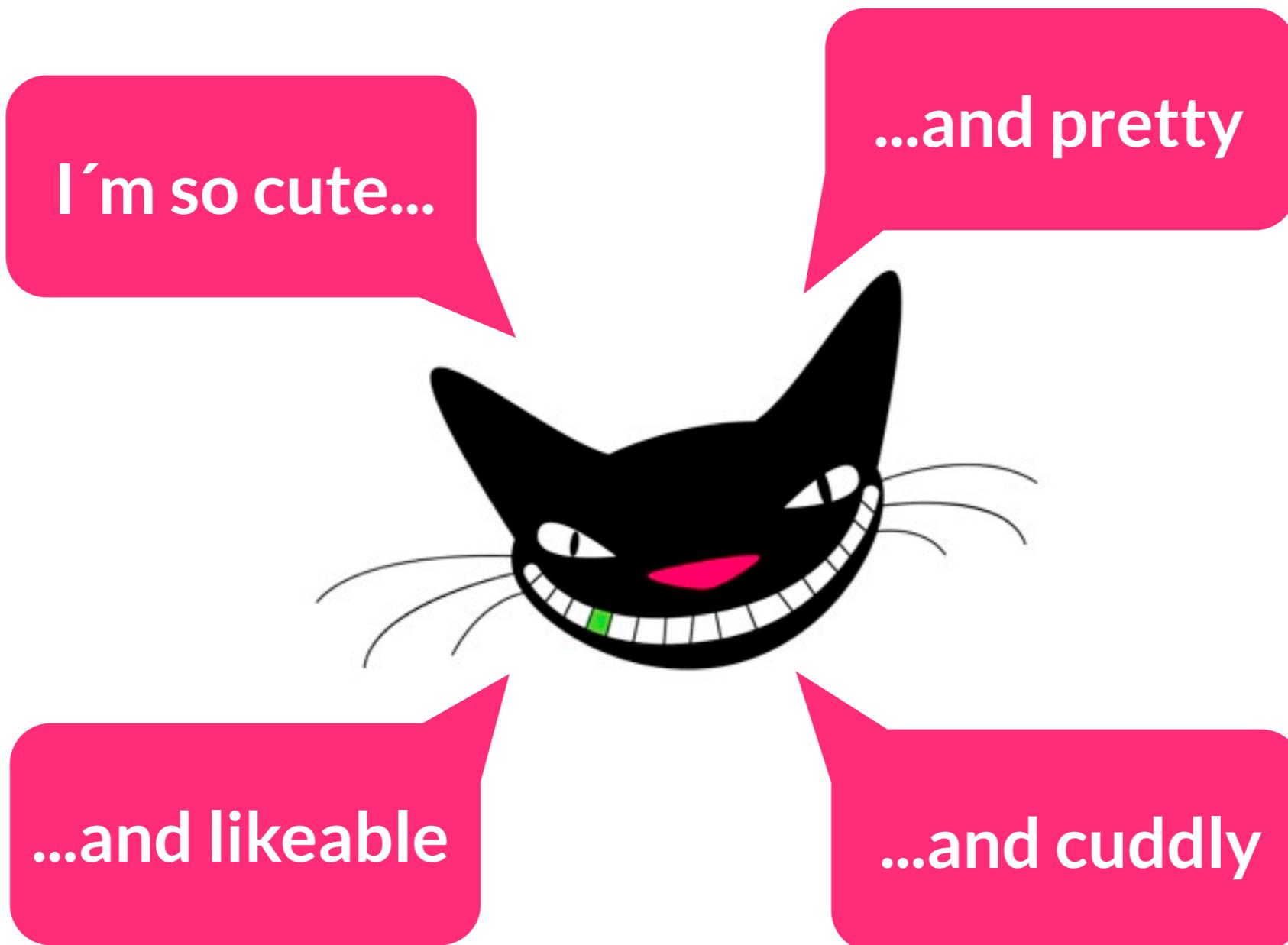
Usability

- ▶ Easy setup
- ▶ Nothing changes in the way you use email
- ▶ Keep your mail client, or...
- ▶ ...use kinko webmail
- ▶ Keep your email address





Why you gotta love (using) me



I'm so cute...

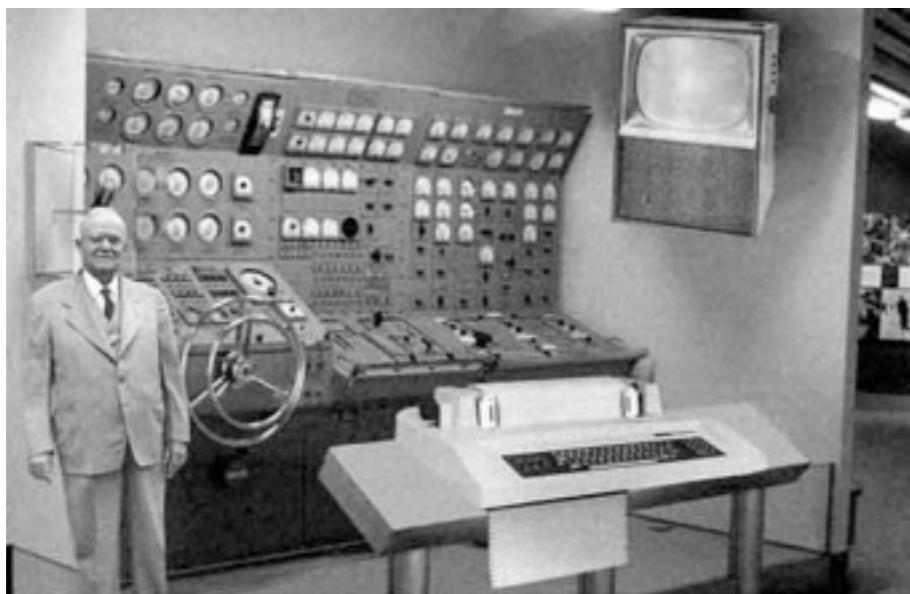
...and pretty

...and likeable

...and cuddly

Challenge: Mobility

- ▶ Yesterday: one person = one computer
- ▶ Today: one person = several computers, phones, tablets, toasters...



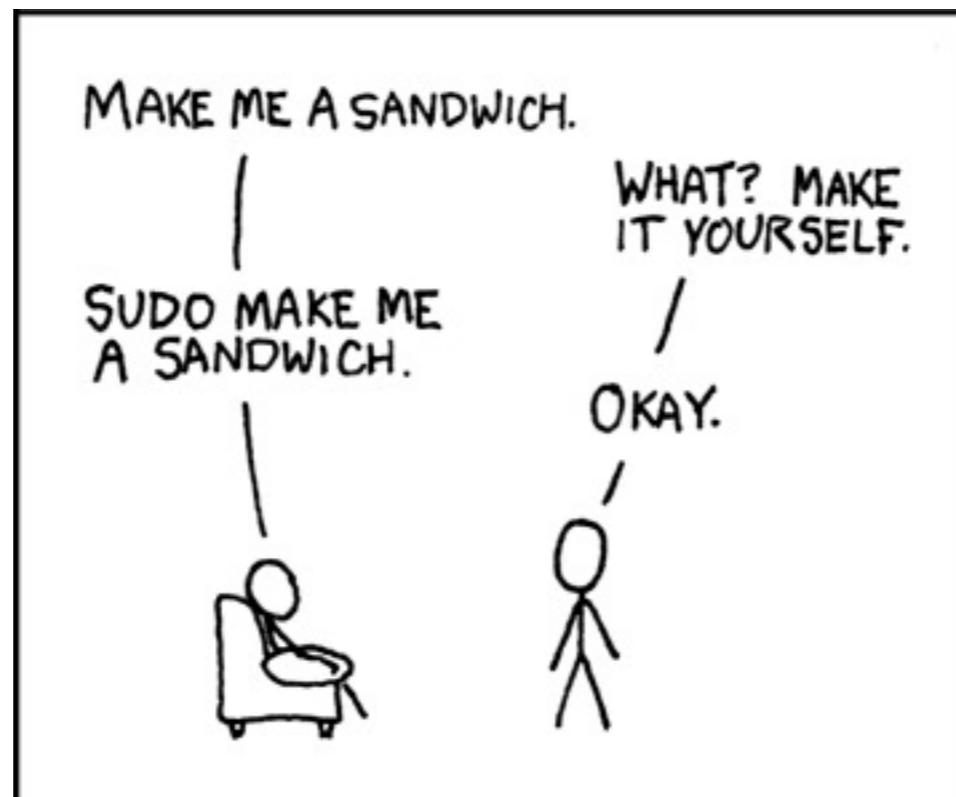
Mobility



- ▶ A proxy in extra hardware
- ▶ with all your devices (Android, Linux, iOS, OSX)
- ▶ accessible from everywhere
- ▶ using default protocols (IMAP, SMTP, Browser)
- ▶ secure connection via port forwarding & SSL certificates

Challenge: Desktop OS

Everyone is root. Everything is perfectly fine!



Challenge: Desktop OS

- ▶ Installation as root
- ▶ Complex operating systems and software
- ▶ Browsers are more and more complex
- ▶ → many potential vulnerabilities

Desktop OS challenges

- ▶ A dedicated device for crypto
- ▶ Minimal, Linux based OS
- ▶ Components secured against each other
(different accounts, etc.)
- ▶ Optional: access to configuration available
only from local network

Challenge: Identity (Key Exchange)

Whom are you talking to?



Challenge: Identity (Key Exchange)

Whom are you talking to?



Identity: technical approaches

- ▶ TOFU: parsed from emails
- ▶ Key server
- ▶ Fingerprint verification

Identity: social approaches

Out of channel verification

- ▶ Identity verification (PostIdent)
- ▶ Signing Service (e.g. heise.de key signing)
- ▶ Web of trust (key signing party)
- ▶ Pseudonym: Business card with email address and fingerprint
- ▶ add your idea here..

Challenge: Trust

Do you trust your mail provider?



Hotmail®



YAHOO! Mail

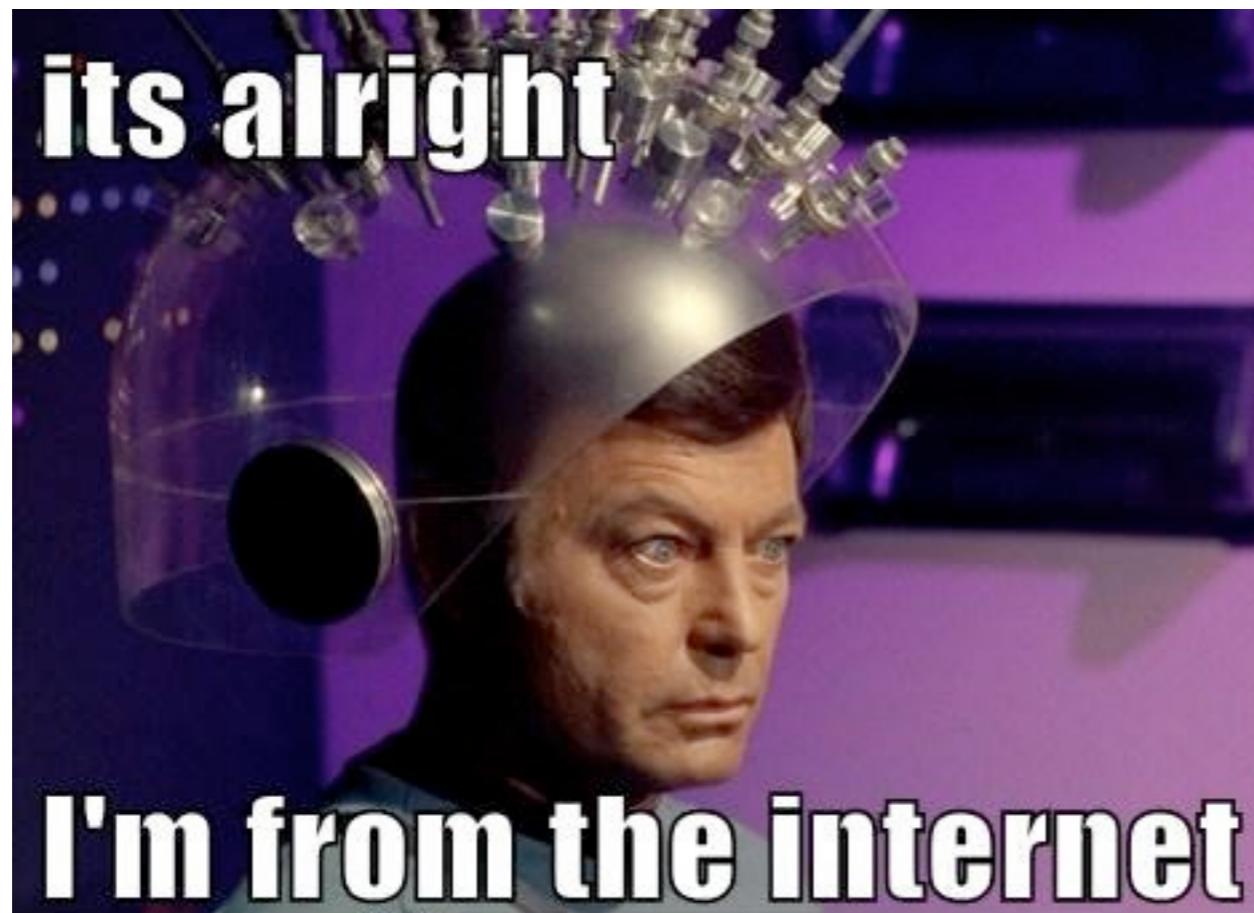


Trust

- ▶ sensitive information (private keys) must be in the user's hands only!
- ▶ tools must be Open Source and reviewed

Challenge: Security

Do you trust us to be masters of math? Would you trust our home made cryptography?



Security

- ▶ use trusted tools like GnuPG
- ▶ stay up to date with security developments
- ▶ keep tools up to date
- ▶ build a vibrant community



More Than Tools



Challenge: Community

A vibrant community is key for a good crypto project.

But how to get people enthusiastic to support your project?

Community

- ▶ Licenses
- ▶ Approachable source code and project organization
- ▶ Communication Tools
- ▶ Newsletter
- ▶ Contributing must be fun!



<https://github.com/kinkome/>



Challenge: Fun

Fun with cryptography.



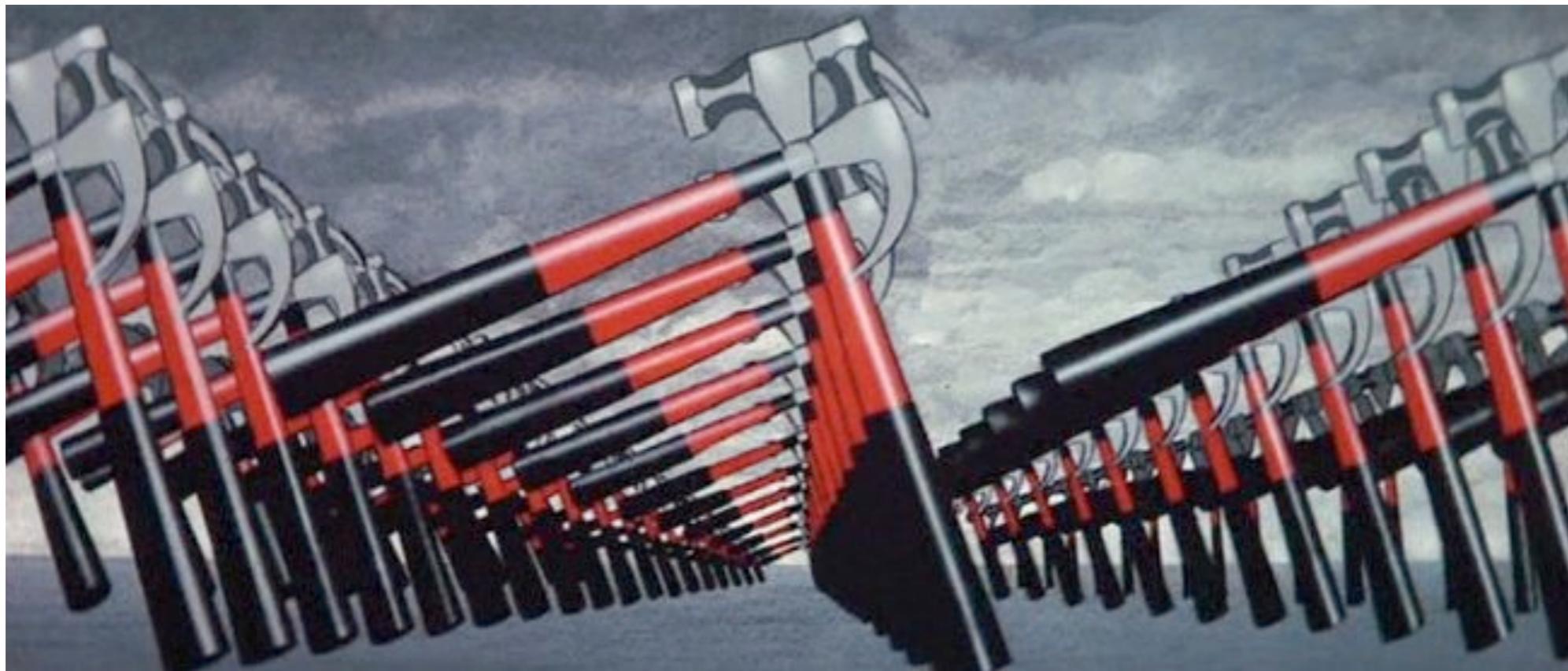
Fun

I think, we've managed so far...



Challenge: Reaching out!

I don't need crypto, I've got nothing to hide!



Reaching out!

- ▶ engage people in conversation
- ▶ use social media as a weapon
- ▶ use educational videos
- ▶ use educational games
- ▶ cause scandals



Challenge: Funding

- ▶ privacy projects need to stay independent of corporate funding
- ▶ so how to cover the costs?

Crowdfunding

- ▶ Crowd Funding for kinko in August
- ▶ independent source of income
- ▶ a means to reach people and media attention
on privacy
- ▶ please back kinko in August!



<https://kinko.me/crowdfunding>



Get involved!

- ▶ subscribe to our newsletter at <https://kinko.me>
- ▶ spread the word
- ▶ contribute to the code
- ▶ help educate the public about privacy
- ▶ contribute with whatever you are best in
- ▶ back us in August

THE FUTURE IS ENCRYPTED