

Security professionals: the plumbers of trust

Piotr Cofta

<http://piotr.cofta.net>

TROOPERS₁₂
Make the world a safer place.

We are the plumbers of trust

WHAT THE !#*\$? ...



- What does a plumber do?
 - brings water from where it is abundant
 - delivers it where it is scarce
- What do we do?
 - bring trust from where it exists
 - deliver it where it is needed

The lock and the key

- You do not have trust in your neighbourhood
- But you trust a locksmith
- So you fit in a new lock
- You just imported some trust from the place where it is abundant (locksmith) to the place where it is missing (neighbourhood)

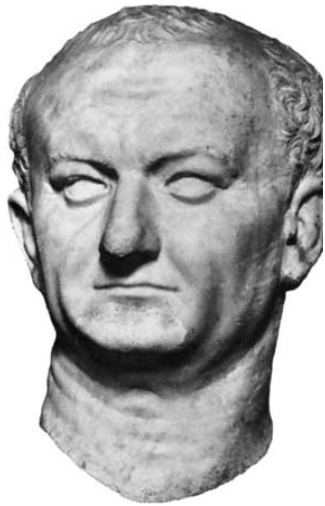


Still not believing it?

- Firewalls
 - no trust in data source
 - but trust in the appliance
- Remote management
 - no trust in the user
 - but trust in the management software
- Signed software
 - no trust in the distribution channel
 - but trust in cryptography



Shooting gallery



pragmatic plumber

Vespasian



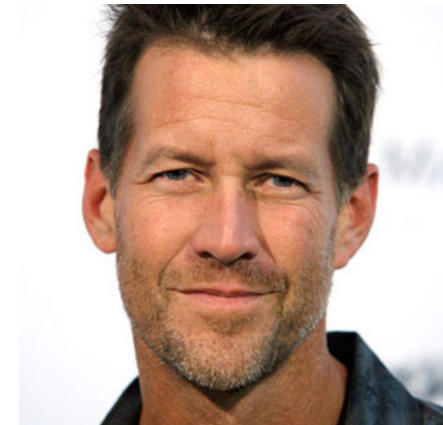
heroic plumber

Mario



guerrilla plumber

Robert de Niro
"Brazil"



sexy plumber

James Denton
"Desperate Housewives"

Why am I here?



- Enno invited me :)
- Plumbers have to know about
 - tools of their trade
 - water
- Most security merchants made their business selling you security **tools**
- I made my business knowing about “**water**” - i.e. about **trust**
- read Luhmann!



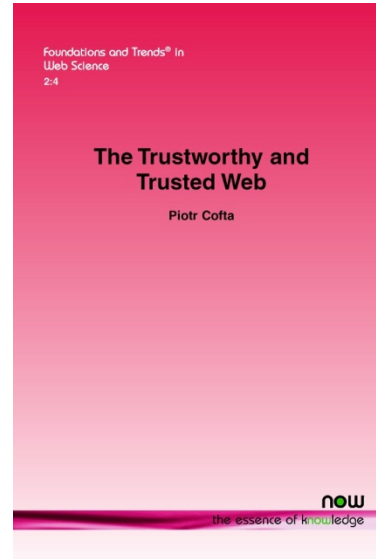
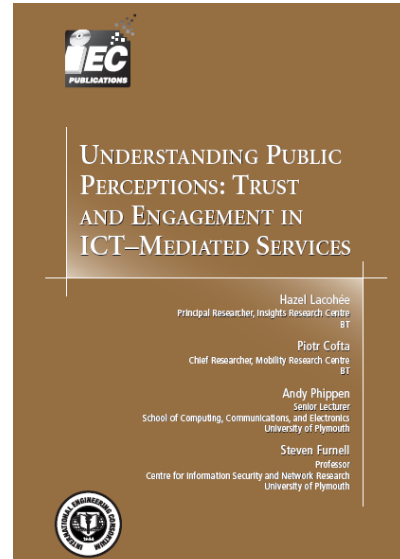
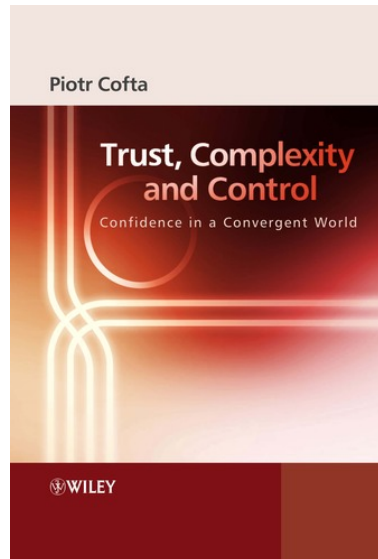
If that's a excuse

Piotr Cofta

PhD CISSP SIEEE

Risk and Trust

<http://piotr.cofta.net>



For today



- What are we talking about
- Canonical structures of trust
- Heuristics of trust

What are we talking about?

(defining trust without feeding the trolls)

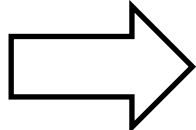
We are all experts in trust

Intention

'I want the
positive future'

Distinction

'I know what
is positive'

Trust is ...  **a state of mind**

Justification

'I have reasons to
justify my intention'

Realisation

'I am dependent on
others'

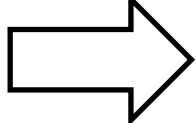
We are all experts in trust

Intention

'I **fear** the
negative future'

Distinction

'I know what
is positive'
(assets)

Risk is ...  **a state of mind**

Justification

'I have reasons to
justify my intention'
(threats)

Realisation

'I am dependent on
others'
(vulnerabilities)

Trust is fashionable..



- Survival skill
 - those who do not 'get' trust, die
 - even banks (some of them)
- Commercial value
 - trust == x £\$€..
 - measurable benefits
- Foundation of security
 - especially information security
 - not the other way round

Trust is, of course, subjective

- 'Your' trust is not always 'my' trust
- What is a 'reasonable' trust is continuously negotiated
- There are some common best practices
- Sometimes even written down
- Better follow them
- Or you face extinction



Trust is, of course, contextual

- Trust your doctor with your surgery, not with fixing your car
- Trust your banker with your money (?), not with your life
- Trust a child with a penny, but not with a pound
- Trust yourself if you are an expert, not if you think you are one



Trust, of course, is *not* transitive

- Trust your friend with fixing a computer security issue



- does NOT mean
- Trust your friend with knowing a reputable information security professional

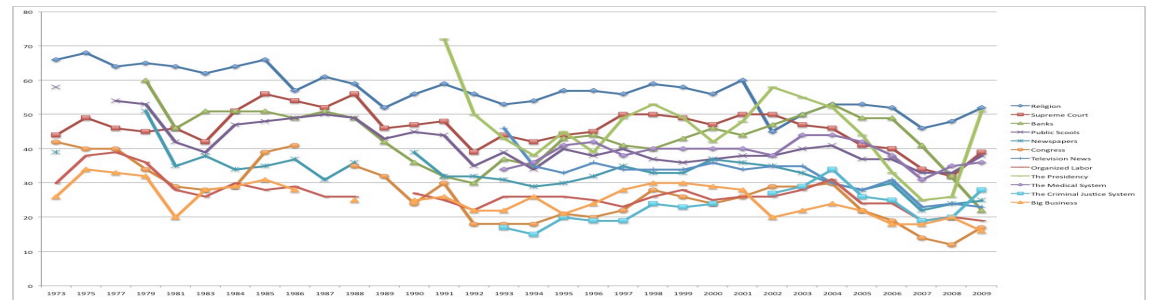
Trust is, of course, context-transitive. But that is a different story.

Trust, of course, changes

- I trusted you, but not anymore
- I did not trust you before, but now I do

If ($Rep(S_i, m-1) \geq NewRep(S_i, m)$)
 $Rep(S_i, m) = \alpha \times Rep(S_i, m-1) +$
 $(1 - \alpha) \times NewRep(S_i, m)$
Else
 $Rep(RS_i, m) = (1 - \alpha) \times Rep(RS_i, m-1) +$
 $\alpha \times NewRep(S_i, m)$

4376-1332-5031-8875-7157



- There is no exact formula
 - "first impression stays"
 - "last impression weights the most"
 - "it is the frequency that counts"

Trust, of course, is *not* reputation

- I trust you **because** of your reputation
- I trust you **despite** your reputation



- Reputation
 - collective assessment of trustworthiness
 - invitation to trust
 - control of one's behaviour
 - long-lasting, valuable asset

Canonical structures of trust

(structuring the piping of trust)

Why do you trust?



- 'Just because I do' is not good enough
- Trust is not about feelings and fluff
- Trust has a rational structure
- But it is often hidden
- Like plumbing is hidden in the walls

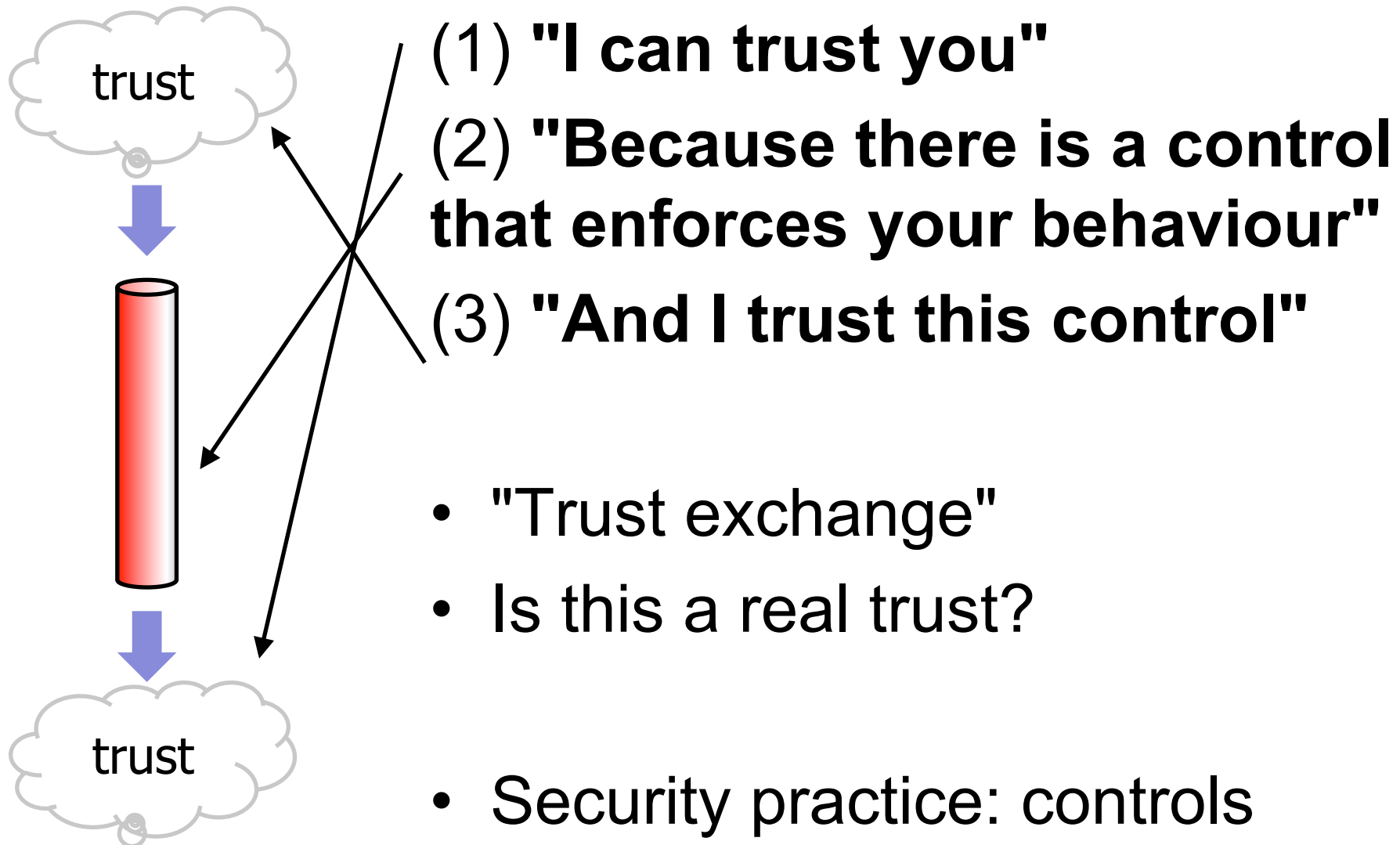
Canonical structures

4376-1332-5031-8875-7157

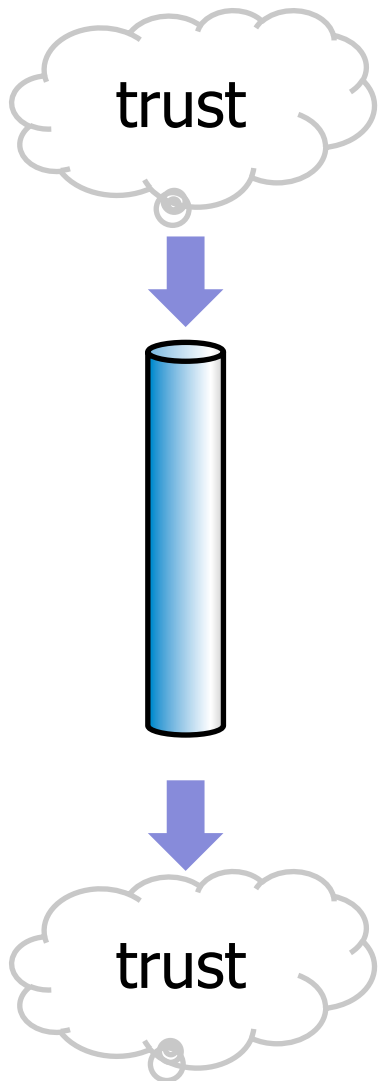


- Even the most complex plumbing has its logic
- Five canonical components of the structure of trust (yours, mine, everybody's)
- Yes, there is a formal notation;
- No, we will not go into it.

1. Control-based trust



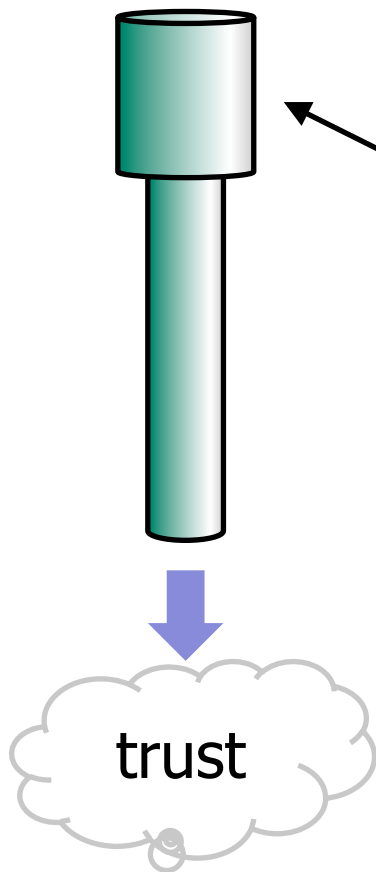
2. Authoritative trust



- **"I trust you because the authority said that I can trust you, and I trust this authority"**
- Institutional trust
- Symbols of trust (certificates, money)
- Institutional reputation
- Security practice: assurance

3. Knowledge-based trust

- I trust you because I know you and I trust myself



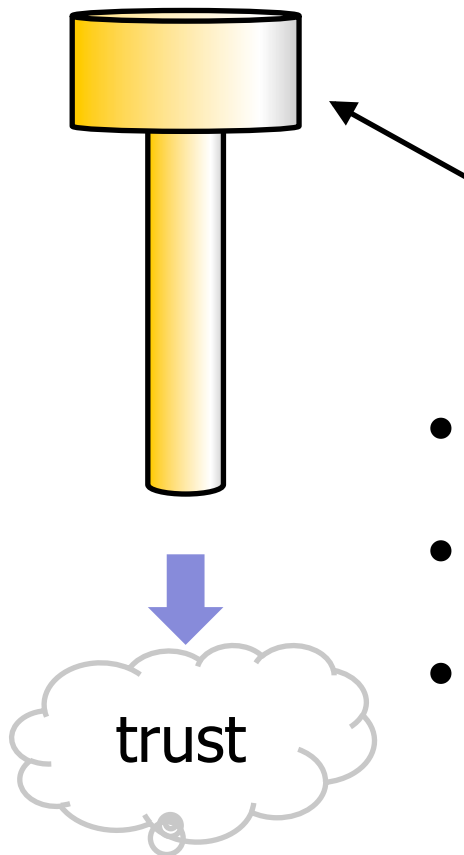
Root of trust #1: myself

- Interpersonal trust
- Personal trust assessment
- Security: personal judgement



4. Consensus-based trust

- I trust you because everybody else seem to trust you



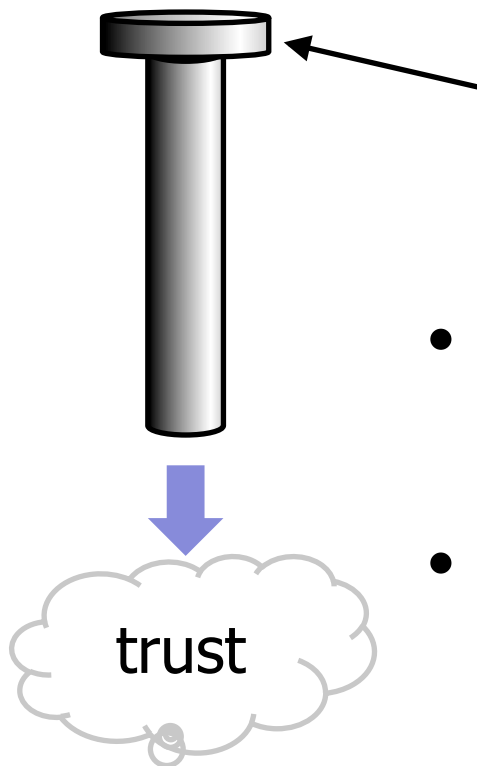
Root of trust #2: the society

- Safety in numbers (like lemmings)
- Social consensus
- Security: best practice



5. Policy-based trust

- I trust you because the policy says I should trust you

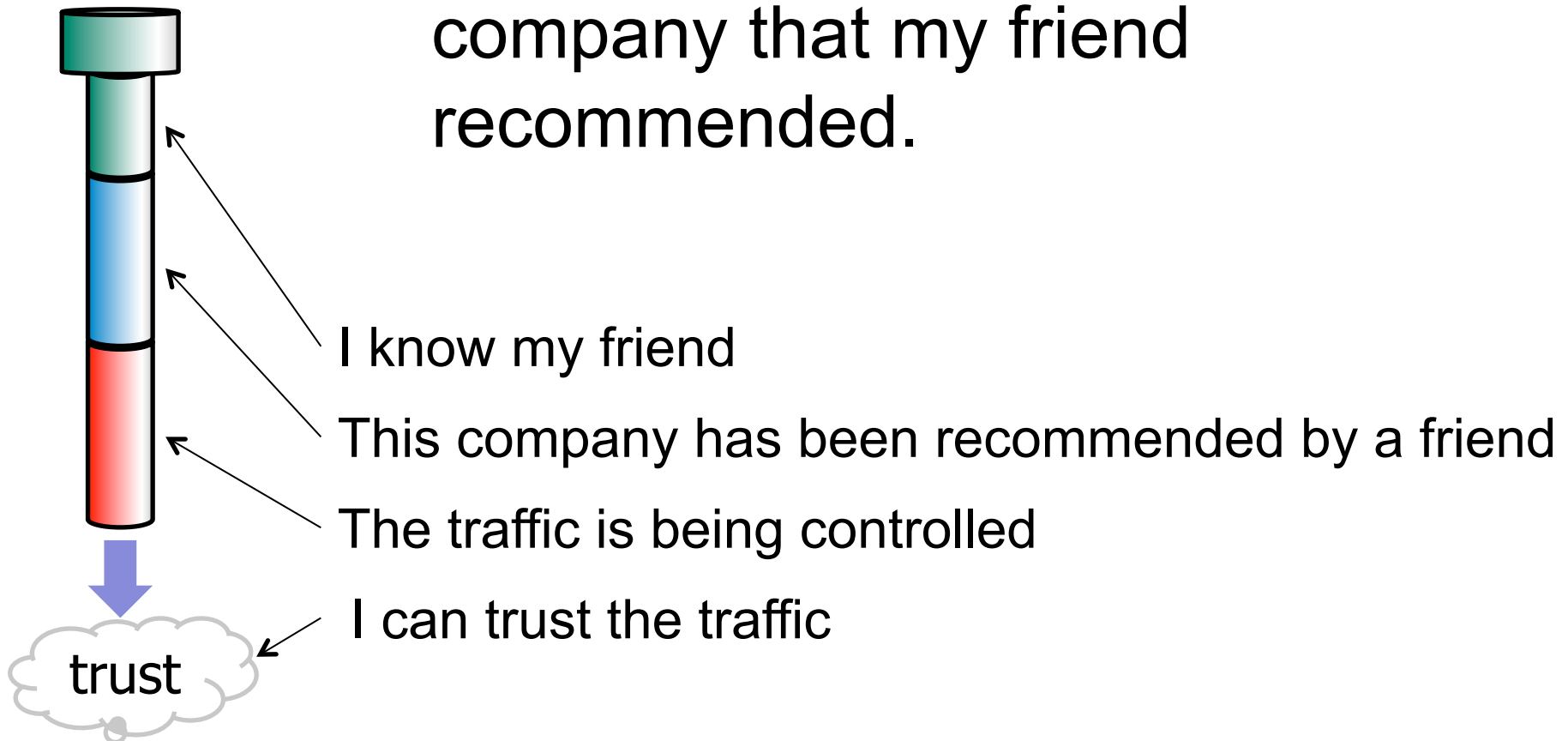


Root of trust #3: CEO

- Works only in closed systems (e.g. company), not in the world society
- Security: trusted systems

Firewall

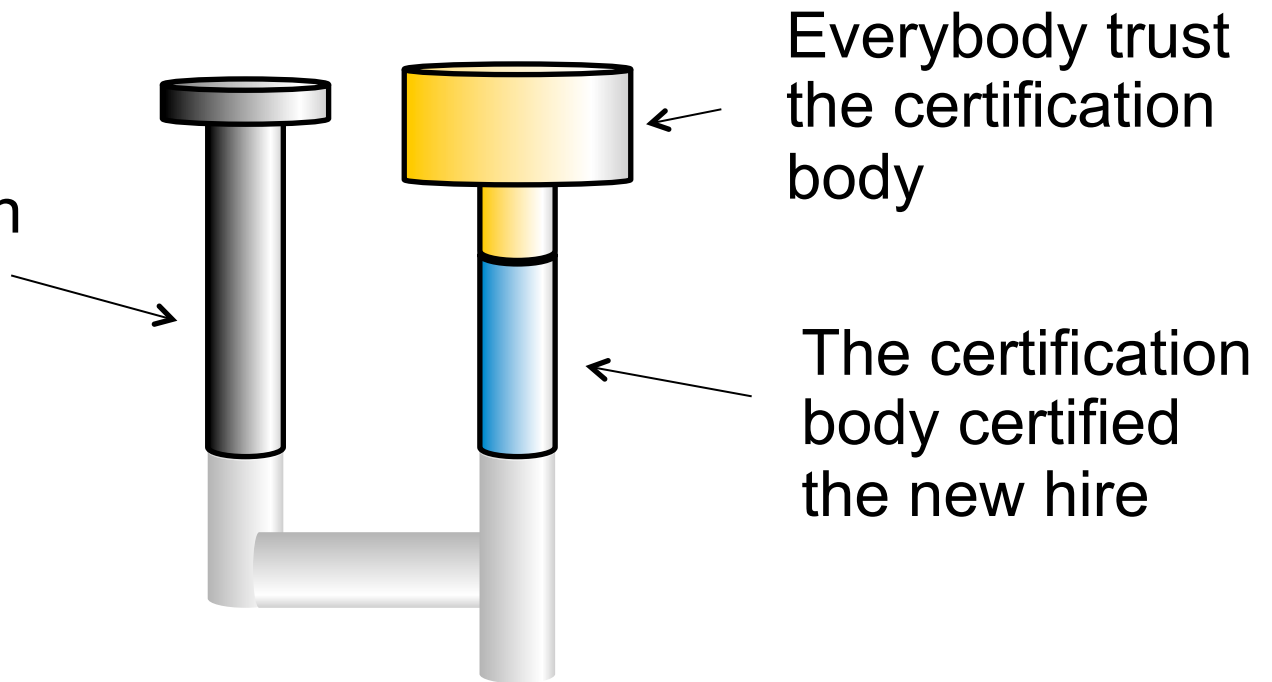
- I could not trust the Internet traffic, so I installed a firewall from a reputable company that my friend recommended.



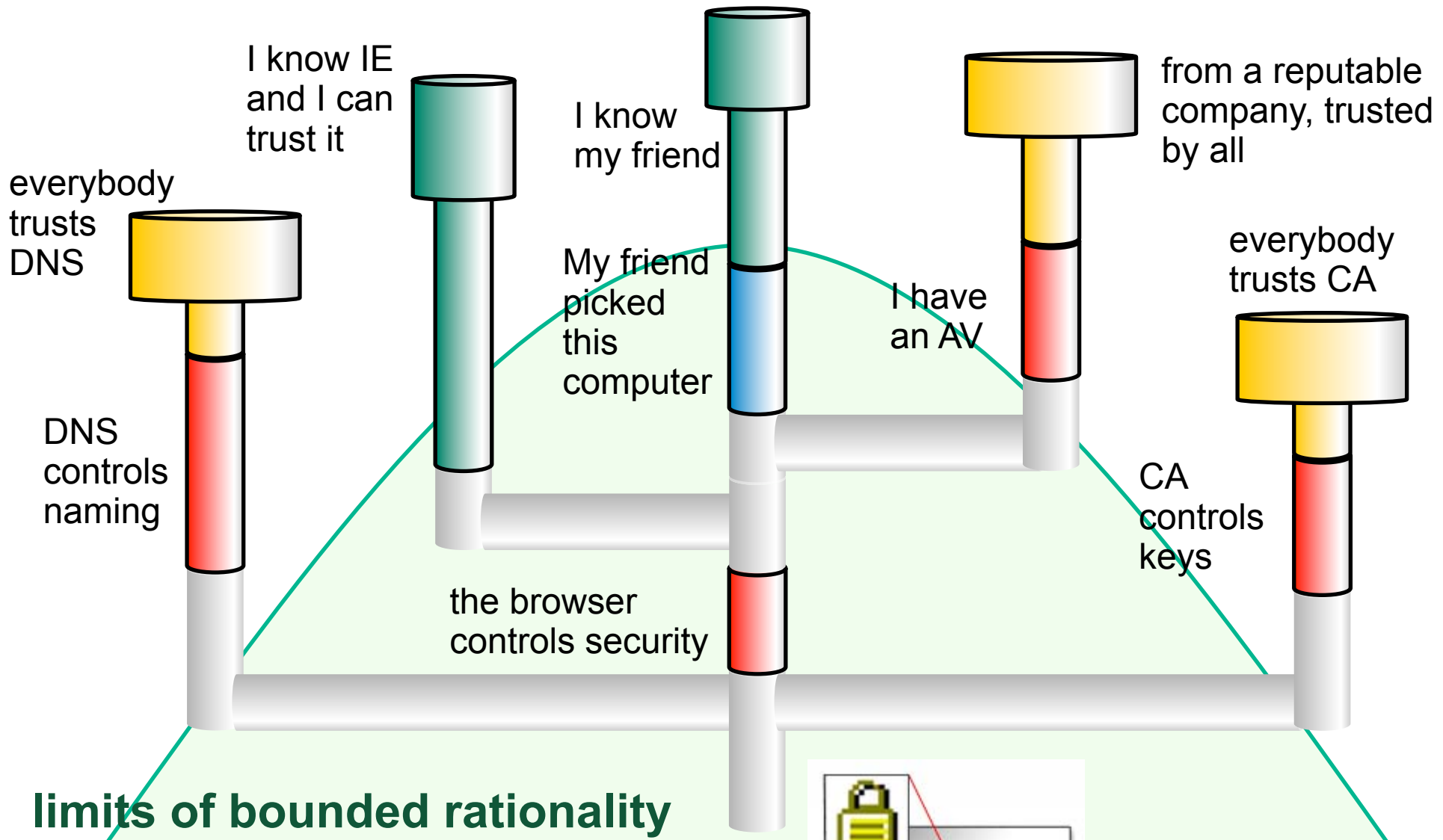
New hire

- I feel safe as we have just hired a new certified security manager

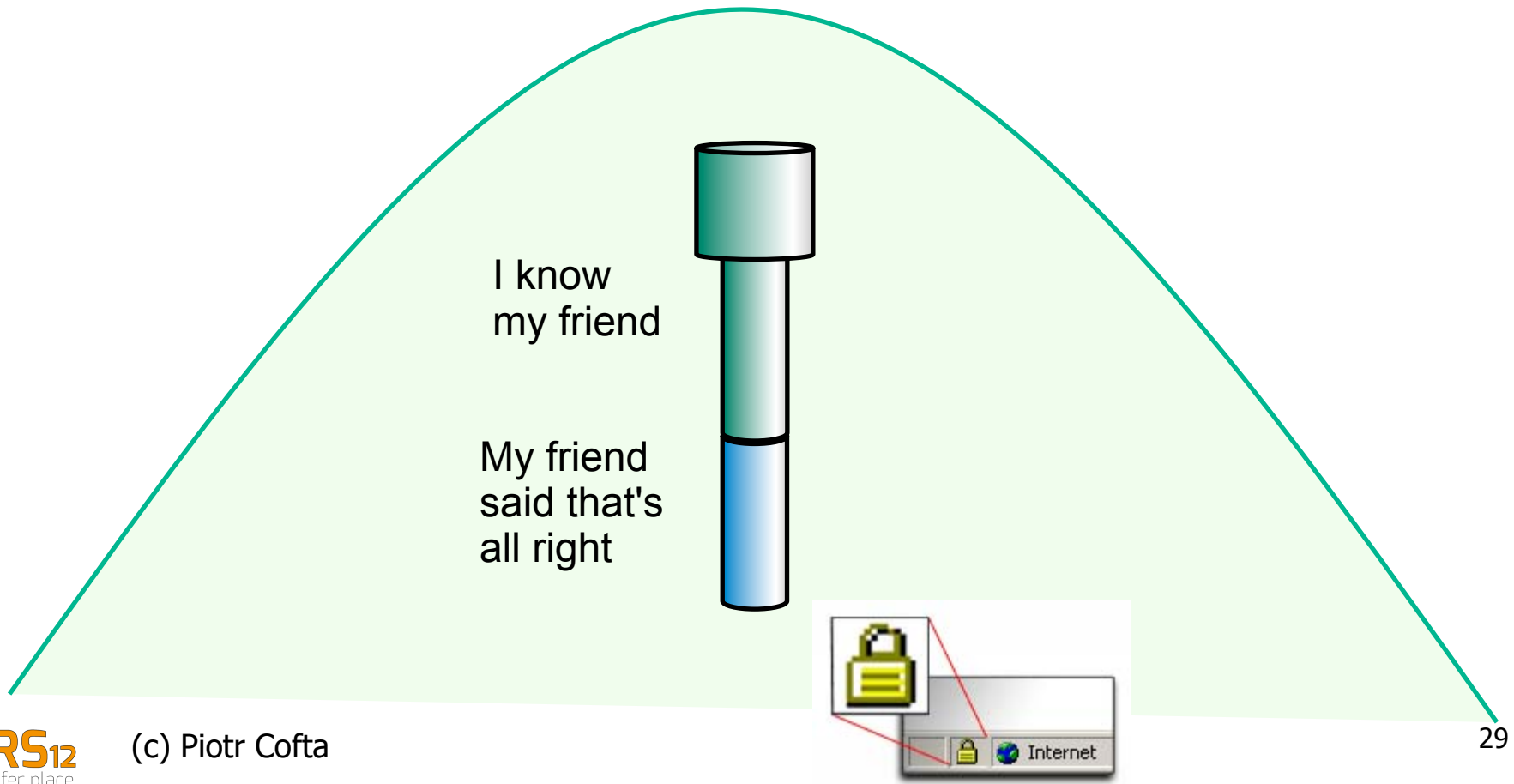
The policy says that we can trust a person with recognised certification



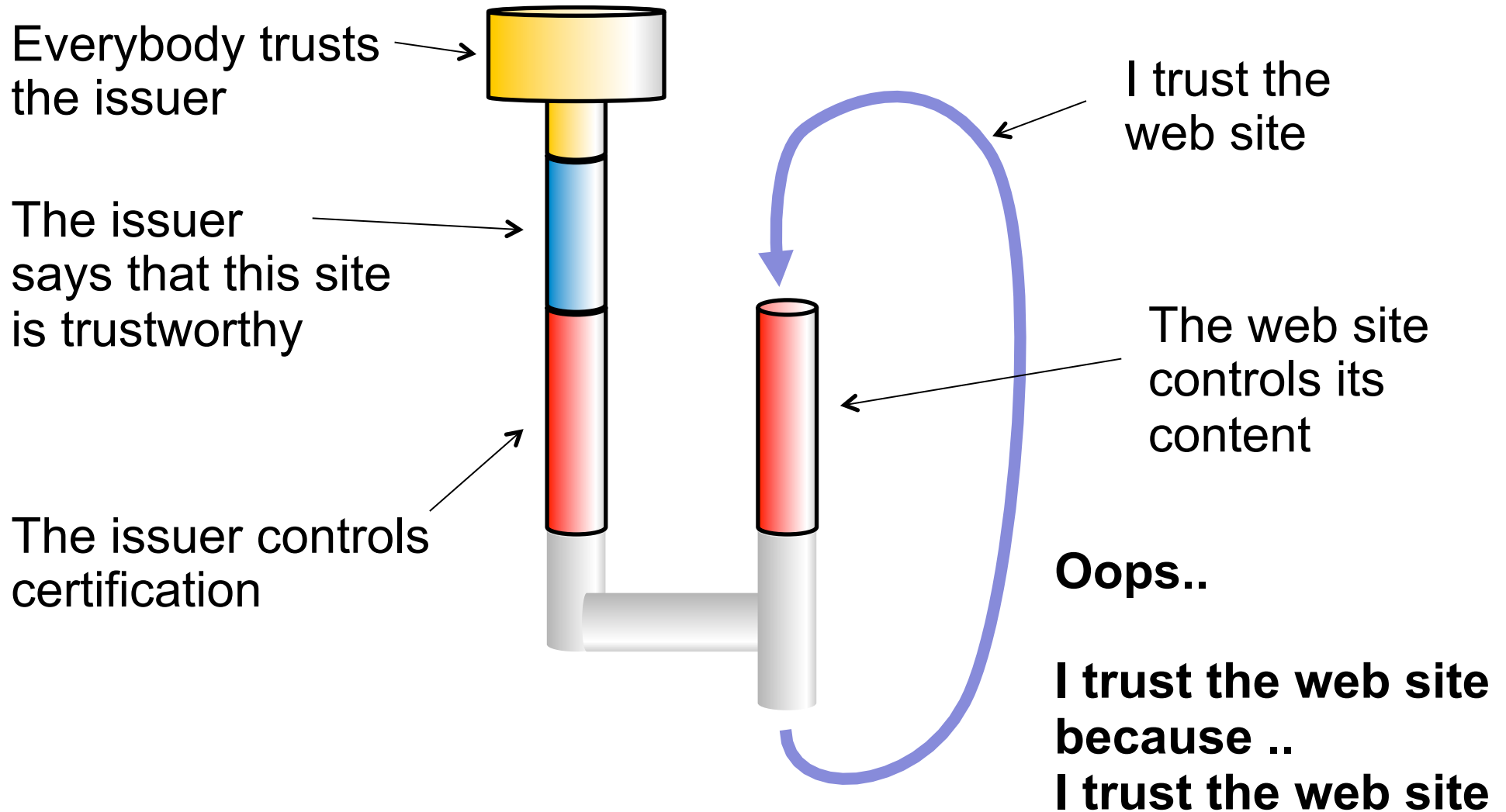
Padlock - the theory



Padlock - the practice



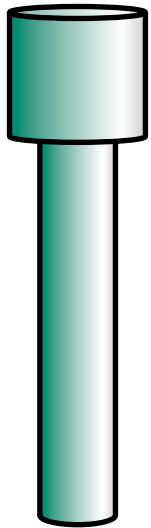
Trust seal



Heuristics of trust

(I trust because I know
.. or..
structuring the green pipe)

Knowledge-based trust



- 'I know' can be a very poor indicator
 - or a very good one
- People do not 'do' perfect logic
 - bounded rationality
- People 'do' survival heuristics
 - just good enough to muddle through
- Security is not an abstract game
 - it is to assure survival over competitors

Heuristics of trust

- Trusting is not an exact science
- Some heuristics are more popular than others

Three-by-three matrix



- **Not** an exhaustive list
- **Never** an exhaustive list

Classical triad



- Competence

- He is **able** to help me, he is a professional

Benevolence

- He seems to be a good man, he **will** not leave me alone

Continuity

- He is really committed, his **future** career is at stake

Sharing triad

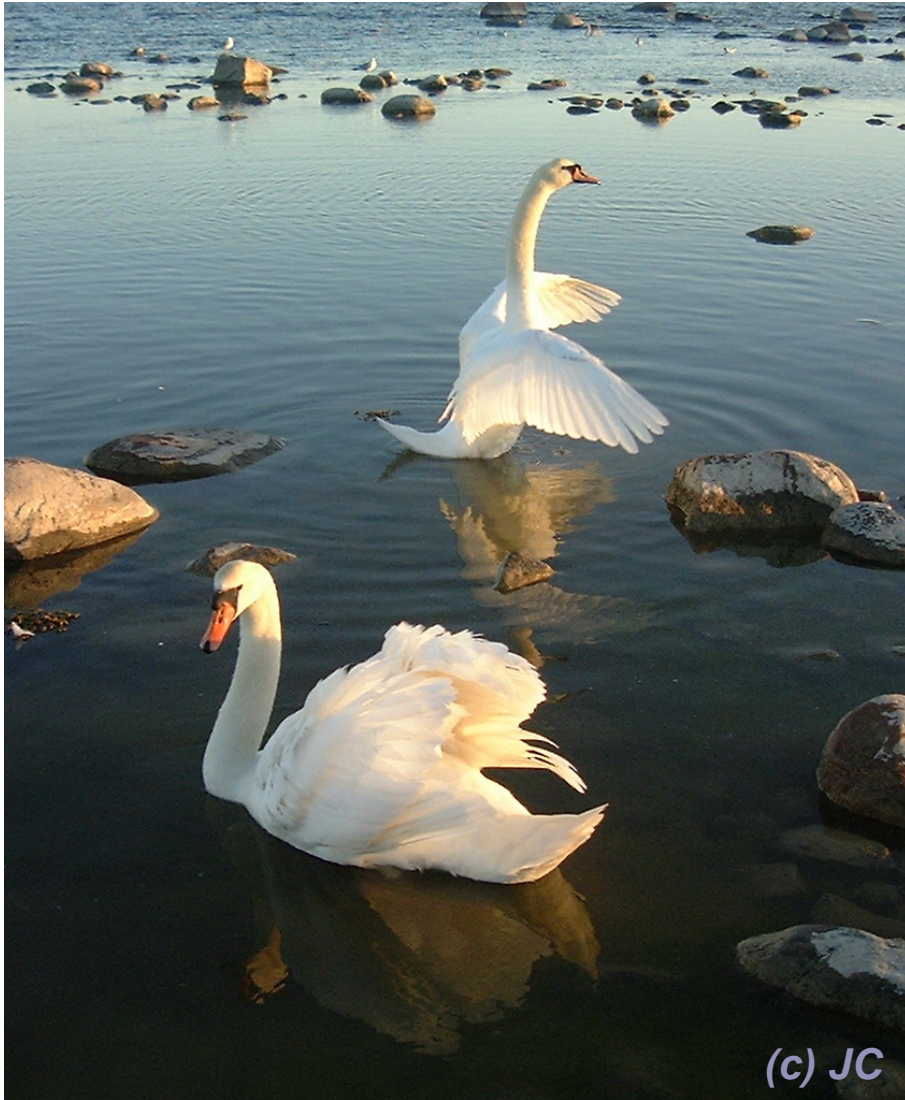
- Shared **background**
 - We are from the same school so I understand him
- Shared **benefits**
 - He is as much dependent on me as I am on him
- Shared **values**
 - We both observe the same fundamental values



Social triad

- Familiarity
 - He is always on time, so he will be on time this time
- Stereotyping
 - Doctors are trustworthy, and he is a doctor
- Similarity
 - I was in a similar situation before and it worked for me





Thank you

Piotr Cofta

<http://piotr.cofta.net>