

PKI Business

István Zsolt BERTA
istvan@berta.hu

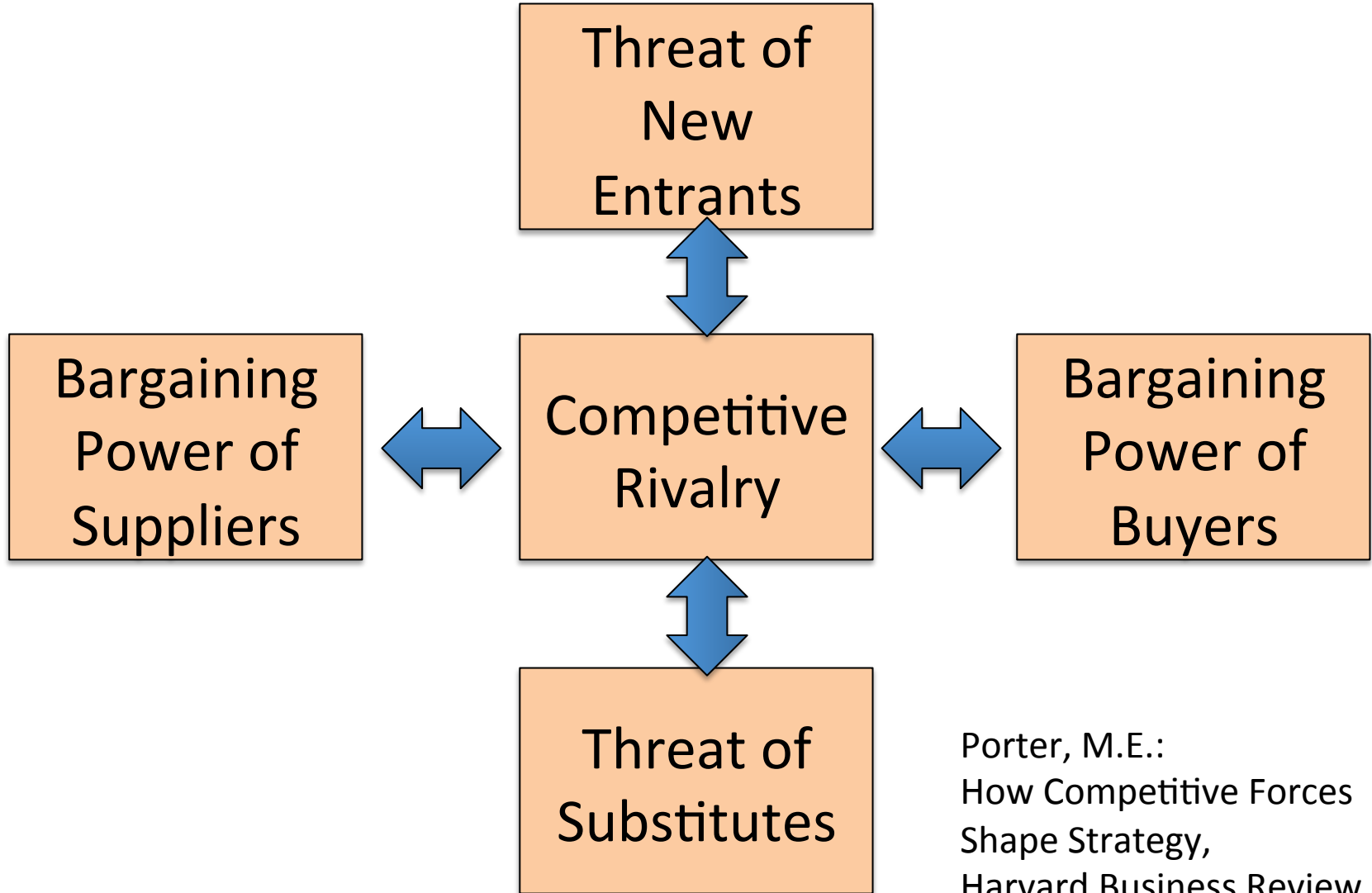
PKI lectures

1. [Public key cryptography primitives](#)
2. [Certificates, Certificate Authorities, Certification Paths](#)
3. [Electronic signatures: signature creation & validation](#)
4. [Information security management at a CA](#)
5. **PKI business**

PKI Business - Contents

- Webserver Certificate Market
- e-Signature Market (EU)
- Substitutes to TLS certs

Michael Porter's five forces



Porter, M.E.:
How Competitive Forces
Shape Strategy,
Harvard Business Review, 1979

DISCLAIMER

- Note: This part of the course will not introduce technology but will be about markets. Opinions will be expressed here, they are not to be confused with facts.

Webserver Certificate Market

Competitive Rivalry

- Global market; any CA is able to issue a cert to any domain
- Business is done mostly on the Internet; geographical location does not matter; regulatory context does matter
- Many (500+) CAs, approx 100-200 of them trusted by apps
 - [SSL observatory's map](#)
- Most of the market (75%) is covered by a few big CAs
 - Symantec, Comodo, GoDaddy
- Massive differences in pricing, weak price competition
 - between USD 1k to free certificates
 - for a very-very similar service
- Market is driven by prestige and brand reputation
- Market players tend to bundle additional services to their certs
- Market players find tend to find creative ways for charging more for essentially the same service

Extended Validation certificates

- Driven by CA/Browser Forum (cabforum.org), agreement between CAs and Browsers/Apps, resulting in:
- Certificate Authorities
 - enforcing certain security best practices
 - enforcing a consistent way for registering end-entities
 - standardizing the way they present information in certs
- Browsers/Apps
 - display EV certs differently (green address bar)
 - display the name of the subject (organization)
- My view:
 - this is beneficial for security in general, this a good solution
 - this is what they should have done at the first place; they just charge more for providing a proper service!
 - financial requirement keep small CAs out of this

Security Seals

- Many CAs provide security seals that can be used on websites
- Clicking on the seals brings you to the CA's site showing that the seal is authentic
- Security-wise they are absolute nonsense; whatever appears on the website should not be trusted when authenticating the site
- There would be point in checking the cert at the CA's site, but not by clicking on the seal
- This is snake oil
- Still, customers often demand these seals...
- They are good tool for branding, but nothing else

Bargaining Power of Buyers

- Buyers cannot differentiate between secure and less secure CAs
- Could become a [market of lemons](#)
- Security-wise, there is no point in selecting a 'good' CA, as the weakest CA's security matters only
 - if one is compromised, the attacker can impersonate any website
- Price and only price should matter (→ [Peter Gutmann](#))
- Still, well-known CAs can charge premium prices
- A cert has relatively little cost for a large organization
- Liability is often dumped on end-users
- **Buyers have relatively little power**

Bargaining Power of Suppliers

- Suppliers include
 - marketing services
 - resellers
 - network providers
 - auditors (e.g. Big4 companies), pentesters
 - hardware and HSM vendors
- As long as a CA can cover a large number of clients, fixed costs become less significant
- If a CA can afford premium pricing, variable costs can be covered easily
- **Suppliers have little power here**

Threat of Substitutes

- What does the product do?
 - secure communication
 - via the Web
 - between parties previously unknown
- Possible substitutes
 - blind trust (and/or hoping that no one attacks)
 - validating yourself that the public key belongs to the website
 - a few tech solutions some geeks can use
- **There is no real threat of substitutes**

Threat of New Enterants

- Setting up a CA is neither hard, nor costly – compared to the size of the market
- The following are really hard:
 - making your roots trusted by all applications
 - establishing a brand known by the customers
- It is often easier to buy an existing CA then setting up a new
- **The market is difficult to enter**
- Many governments do not like certs to be out of their control, so they set up new CAs
- Recent news on mass surveillance and international espionage make this an especially hard problem

Conclusions

- Thriving market
- Intense competition
 - not on price, but
 - on branding and
 - on additional services
- Premium pricing
- Market is hard to enter and there are no real substitutes
- Loss of confidence can be a threat
- Some recent events may decrease confidence while they have little effect on the average user

References/Recommended reading

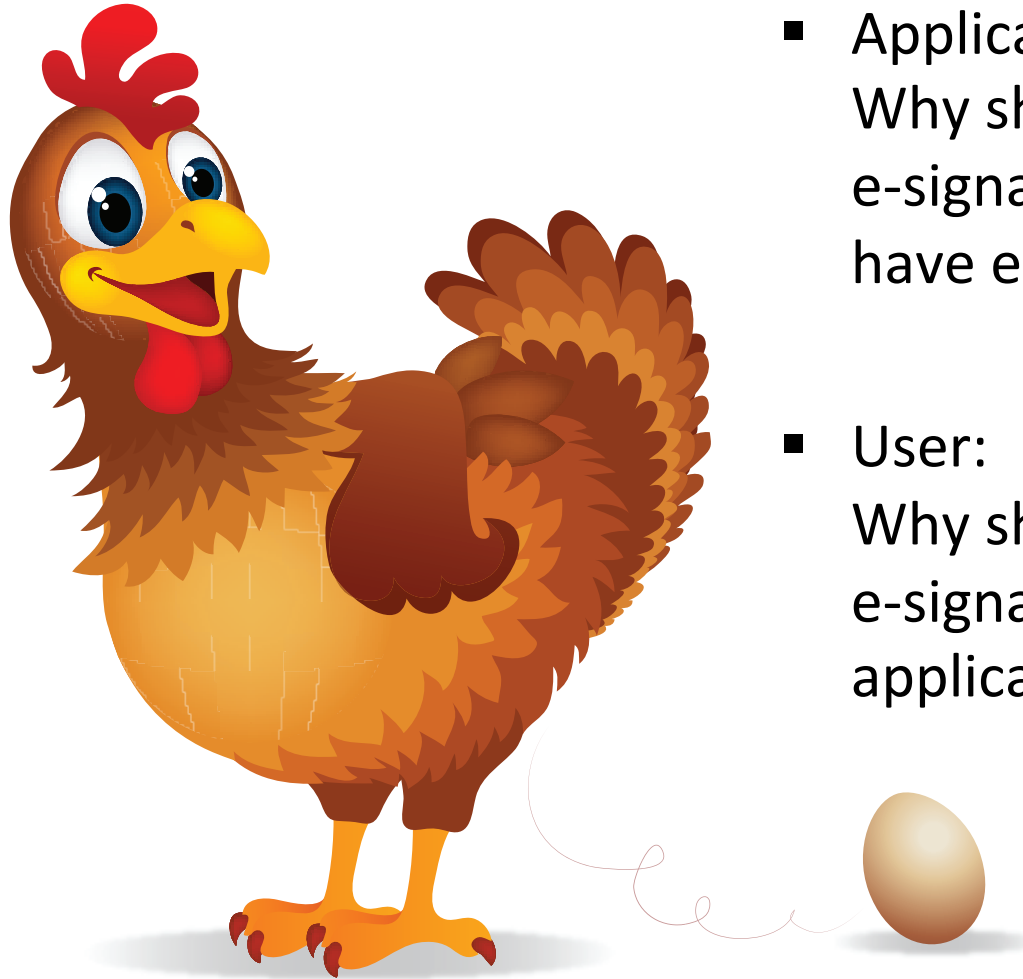
- [Security Collapse in the HTTPS Market](#)
- [EFF SSL Observatory website](#)
- [Why Phishing Works](#)
- [Everything you Never Wanted to Know about PKI but were Forced to Find Out](#)

e-Signature Market

Competitive Rivalry (1)

- There is no single market; there are market niches in different PKI communities in different EU Member States
- It is hard/impossible for a CA in one EU country to enter another
- Any market/niche is artificial, created not by actual demand but by regulations either
 - mandating the use of e-signatures for a certain task
 - allowing e-signatures as a better alternative for a certain task
- Small niches – no economies of scale
- No central oversight/data on niches
- In (almost) all EU Member States the required expertise is concentrated at a few competence centers (companies); their existence depends on the given market niche, any EU-wide competition would conflict with their interests
- Massive dependence on laws and regulations and not on market forces

Chicken and Egg problem



- Application:
Why should I support e-signatures if so few people have e-signatures?
- User:
Why should I buy an e-signature if so few applications support it?

Bargaining Power of Buyers

- Prices depend on:
 - how much does it cost to have an e-signature?
 - at how many places can I use my e-signature?
 - quantity the product is sold
- For any given application, it is generally too expensive to request an e-signature from the client (human end-user)
- Economies of scale and the possibility to use it in multiple applications could allow more penetration
- End-user buyers usually avoid paying for this
- Organizational buyers often wait until this becomes cheaper
- Government would be the main user...

Government as a buyer

- The government (of any EU Member State) would be a primary user of e-signatures
- Governments dictate requirements and work on establishing a market for their special signatures
- However, governmental applications often do not appear or appear without supporting e-signatures
- In case of any massive e-signature application, any government will consider setting up their own CA
- The very possibility of this can paralyze a market

Bargaining Power of Suppliers

- Suppliers
 - vendors of software / hardware / infrastructure / SSCDs
 - auditors / pentesters
 - registration service? (though generally not viable)
 - sales+marketing costs
- As qualified signatures must be equivalent with handwritten signatures, security requirements are very high
- The market is small
- Fixed costs dominate, they prevent many CAs from being profitable
- Current markets are too small for certain technology vendors, they are unwilling to adjust their products to the ever-changing regulations; they also have certification costs
- **Market players have little bargaining power over their suppliers**

Threat of New Entrants

- Market niches are very hard, almost impossible to enter from the outside
- High setup costs, profitability is very far away
- Governments can enter this field any time, and kill any existing market either by
 - mandating their certs and locking out any other player
 - pushing certs to people for free
- Large organizational buyers may also consider setting up their own CAs...

What is the added value



Certificate Authority

Hi, I am a CA, I can register your employees, and then you will know who they are.



Customer
(large organization)

Come on, I already know who my employees are. Why would I pay for such a service?

Threat of Substitutes

- Possible substitutes are:
 - paper-based signatures
 - blind trust
 - huge (governmental portals) which are trusted
- Many governments introduce portals instead of signing documents; this does not authenticate documents, but may act as a substitute – this is a **major threat to this market**
- Huge portals - Too big to fail?

How will the new EU regulation change this?

- By removing national regulations, it tries to remove barriers from entering market niches and creating a single market
- If it works, it will eliminate many competence centers in MSs
- I don't think it will be able to create EU-wide competition, governments will not want other countries to have this amount of control over their public administration
- The Regulation did not address the biggest problem of the market, a buyer still has no real way of using their signature...

What is wrong?

Hi, I would like to send you this official document, please find it here, electronically signed.

Officer
at a government
or a company



User with
electronic
signature

Sorry, I accept no electronic documents

Sorry, I do not accept documents/
signatures in the foo format

I want you to use my website instead



Nothing will work as you cannot expect others to accept e-signatures as they accept paper.

Business cases that DO work

- Electronic invoicing, business2consumer
 - e-invoices are significantly cheaper than paper based ones
 - economies of scale can work here
 - timestamping can be a business for PKI providers
 - EU is working to remove timestamping requirements
- Document preservation
 - scan it, sign it, timestamp it, and you can get rid of the original
- Document workflows work very-very rarely only

Document workflows in the Hungarian niche

- Registry of businesses
 - lawyers initiate the registration of a new business in an electronic way
 - registry court judges pass an electronic deed about the company
- Notary publics use electronic signature for archiving notarial deeds
- All financial institutions report changes in bank account numbers of companies to registry country electronically
- Judicial executors query information from financial institutions using electronic signatures
- Lawyers use electronic signatures for querying certain governmental databases
- Some governmental (e.g. land registry, tax authority) institutions issue electronic versions of certain deeds

Summary

- Market niches, very difficult to enter
- Artificial markets, created by regulation
- Driven by regulation not by business
- Government: major threat/opportunity

Substitutes to TSL Certificates

Recent problems with SSL / TLS

- Issues with the security of Certificate Authorities
 - Comodo, Diginotar, KPN, Trustwave, ... (see more info [here](#))
- News on international espionage
 - attacks against CAs
 - [compelled certificate attack](#) (i.e. a government orders a CA to issue a false certificate)
- Weaknesses in the protocol
 - [renegotiation](#), BEAST, CRIME, POODLE, etc.
- Weaknesses in SSL / TLS implementations
 - [gotofail](#), [heartbleed](#), [CSS injection](#), etc.
- Weak keys [in large numbers](#) (0.2% of all keys on the web)

Initiatives for improving CA security

- CA/Browser Forum
 - industry-led attempts to make order and improve security
 - [Baseline Requirements](#)
 - [Network Security Reqs](#)
 - all are very basic requirements
 - how are they enforced?
- New EU regulation replacing the e-Signature Directive
 - more focus on security
 - focus on incident reporting
 - will apply to TLS certificates too (current Directive is for e-signature only)

Regardless of these initiatives...

- Browsers trust all (100+) CAs globally; if one CA is breached, the attacker can impersonate any website
- CAs operate in different countries and jurisdictions, these trust each-other... but to a certain level only
 - Are we trying to establish a trust relationship electronically that does not exist in the real world?
- Commercial CAs
 - will always be driving down costs to stay competitive
 - select the auditor they prefer
- Governmental CAs
 - often do not have a proper, independent audit, but provide an audit-equivalency statement only



Approach: Let's have fewer CAs

- Why are we trusting 100+ CAs, where some are very small and are from distant countries you have never heard of? Most certs are issued by a few global CAs; why trust small ones?
 - Smaller countries would need to rely on security from someone else – will they accept this?
 - Recent news on attacks include:
[Comodo](#), [Verisign](#), [Globalsign](#)...
Hey, these are the big ones!!!
- Still, if you know that you need a few CAs in a certain application only, there can be point in distrusting all others



Approach: Let's restrict the authority of CAs

- Why are all CAs trusted globally? Why are not they restricted to e.g. a country/region, etc?
- Yes, but we now have global CAs – what to do with them?
- Who would be limiting the market and how?
- X.509 has a plethora of tools for this (Name Constraints, Policy Constraints, etc)
 - We are still having problems around Basic Constraints (differentiating CA and end-entity certs) in browsers
 - X.509 path building is VERY complex, hard to do well
- CA/Browser Forum documents allow CAs to constraint themselves voluntarily – browsers do not support it yet
- Still, this could be a way forward...



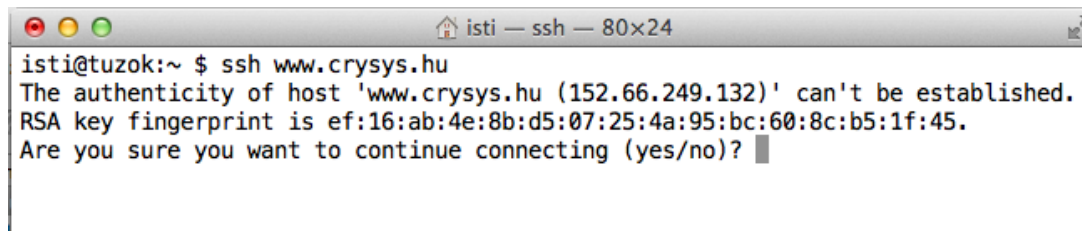
Self-signed certificates

- The connection is encrypted and integrity checks are applied but you do not know who you are connected to
- They provide no protection against man-in-the-middle attacks
- Considered as heresy
- But: Certificates are used when verifying if the given public key belongs to the given entity (web server) only; what if I do this check myself?
 - Example: I receive the cert on a secure channel
 - Example 2: Check cert fingerprint with the counterpart
 - Some people actually [try to do this](#)...
 - Come on, this approach does not scale!!



Approach: Trust on First Use (TOFU)

- First time you receive the key → trust it; but be suspicious when it changes
- SSH uses the same concept – who checks the fingerprint? (yes, but SSH is not used towards arbitrary servers globally)

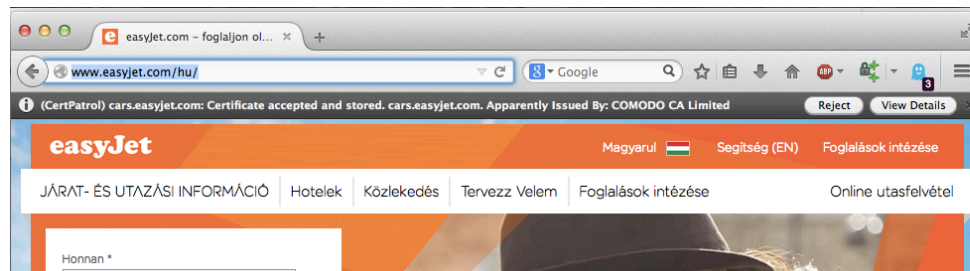


```
isti@tuzok:~ $ ssh www.crysys.hu
The authenticity of host 'www.crysys.hu (152.66.249.132)' can't be established.
RSA key fingerprint is ef:16:ab:4e:8b:d5:07:25:4a:95:bc:60:8c:b5:1f:45.
Are you sure you want to continue connecting (yes/no)?
```

- No protection against man-in-the-middle attacks on first use; but if there is a MITM attack on first use, the attacker must remain in the connection (forever) or risk being detected
- Phil Zimmermann's [ZFone](#) uses a similar approach: [RFC 6189](#)

Tool: Certificate Patrol

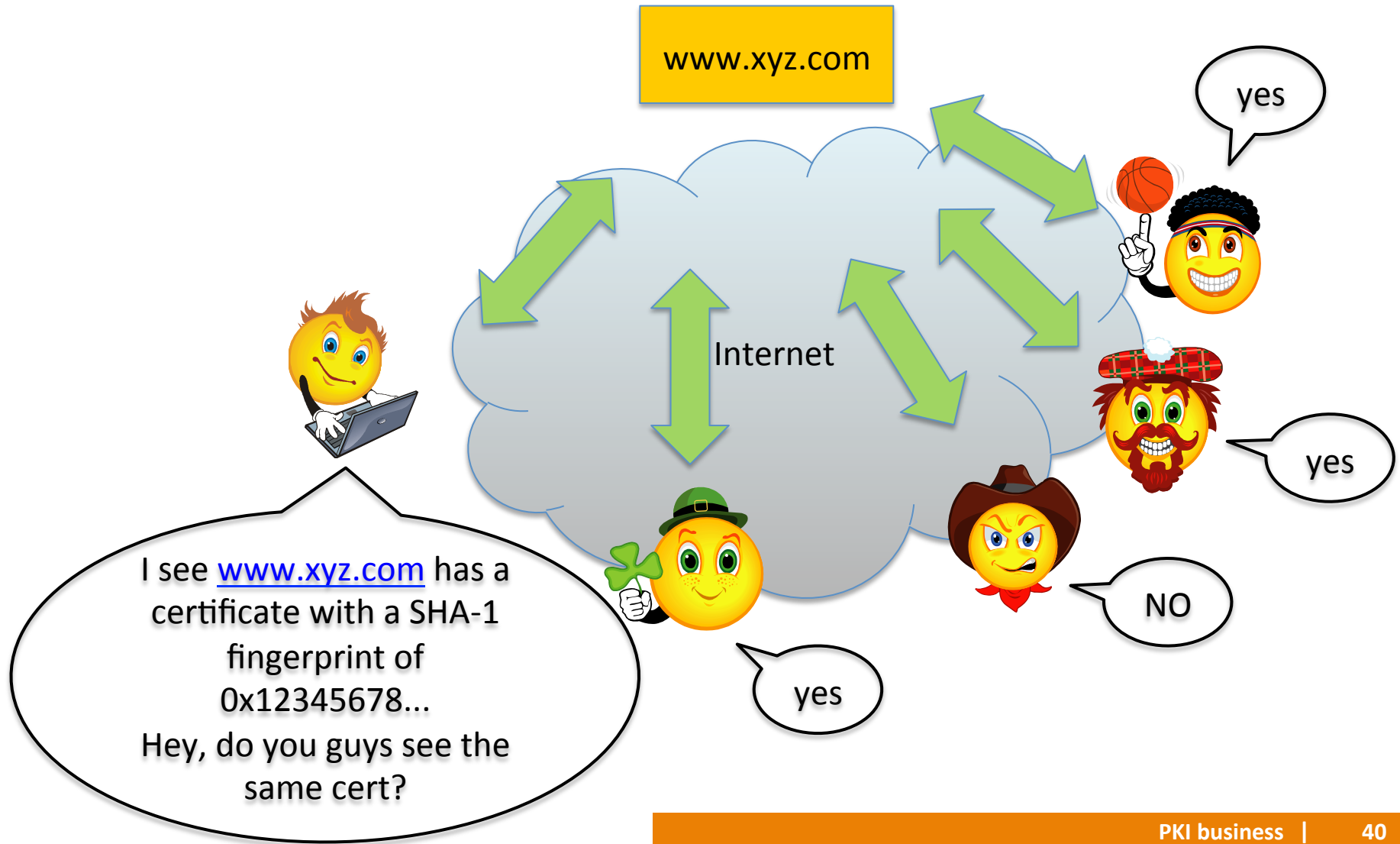
- A [Firefox Addon](#) implementing certificate pinning
- Takes note of certificates of sites you visit
- For known sites, checks if the certificate is known
- Displays a warning message when a site's certificate changes
- Provides a different treatment for low-threat harmless-looking updates (e.g. same key? same CA?)



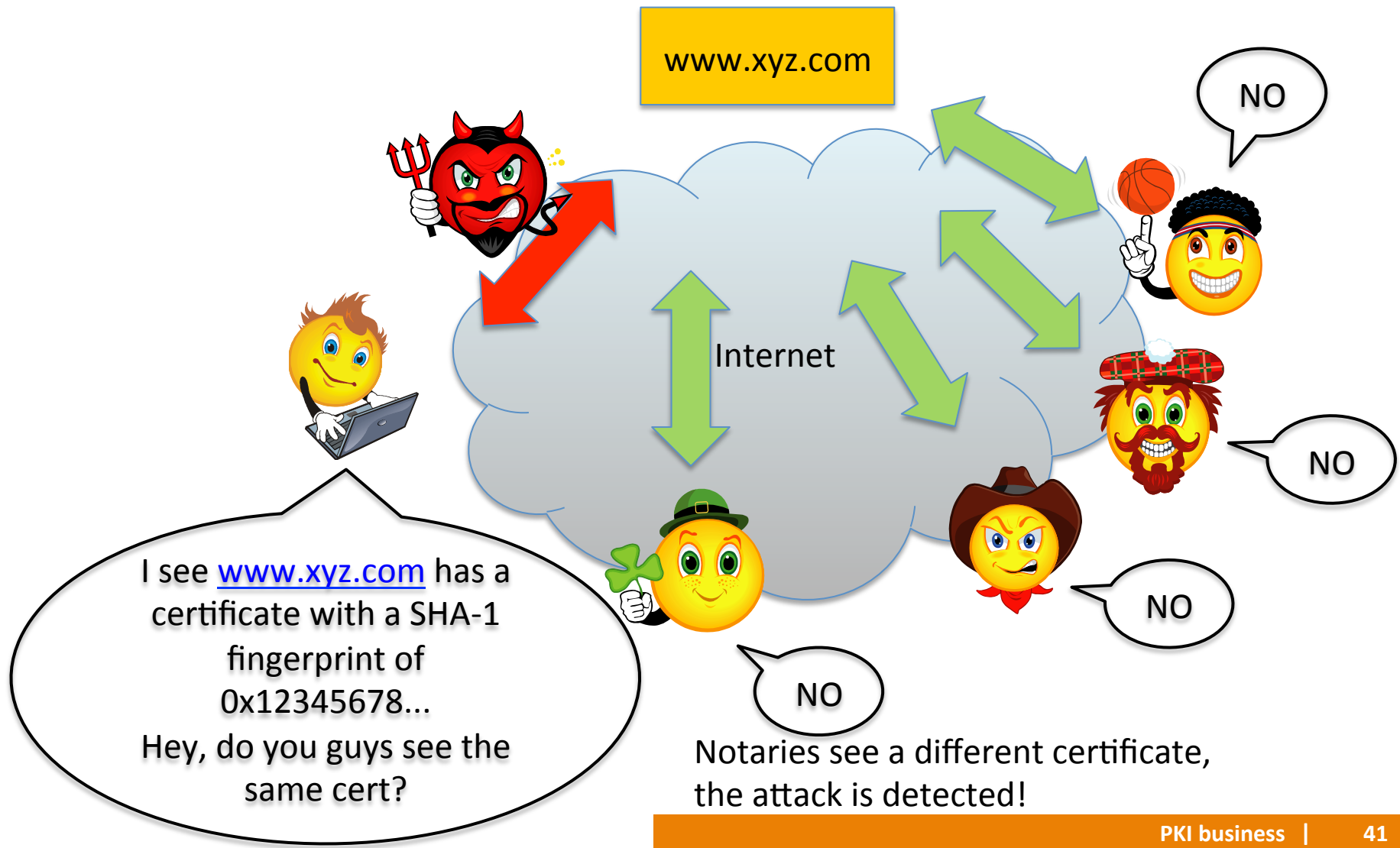
Tool: Perspectives

- Relies on multiple network notaries who continuously monitor public keys used by webserver
- When the client connects to a new website, she contacts some randomly selected notaries and asks what public keys they see
- The website is looked at from different *perspectives*, i.e. by the client and by the notaries
- Uses PGP for protecting communication with notaries
- Also incorporates the TOFU approach, contacts notaries when a key/cert is updated only
- Client is available as [Firefox Addon](#)
- Research paper: [Wendlandt&Andersen&Perrig, 2011](#) (CMU)

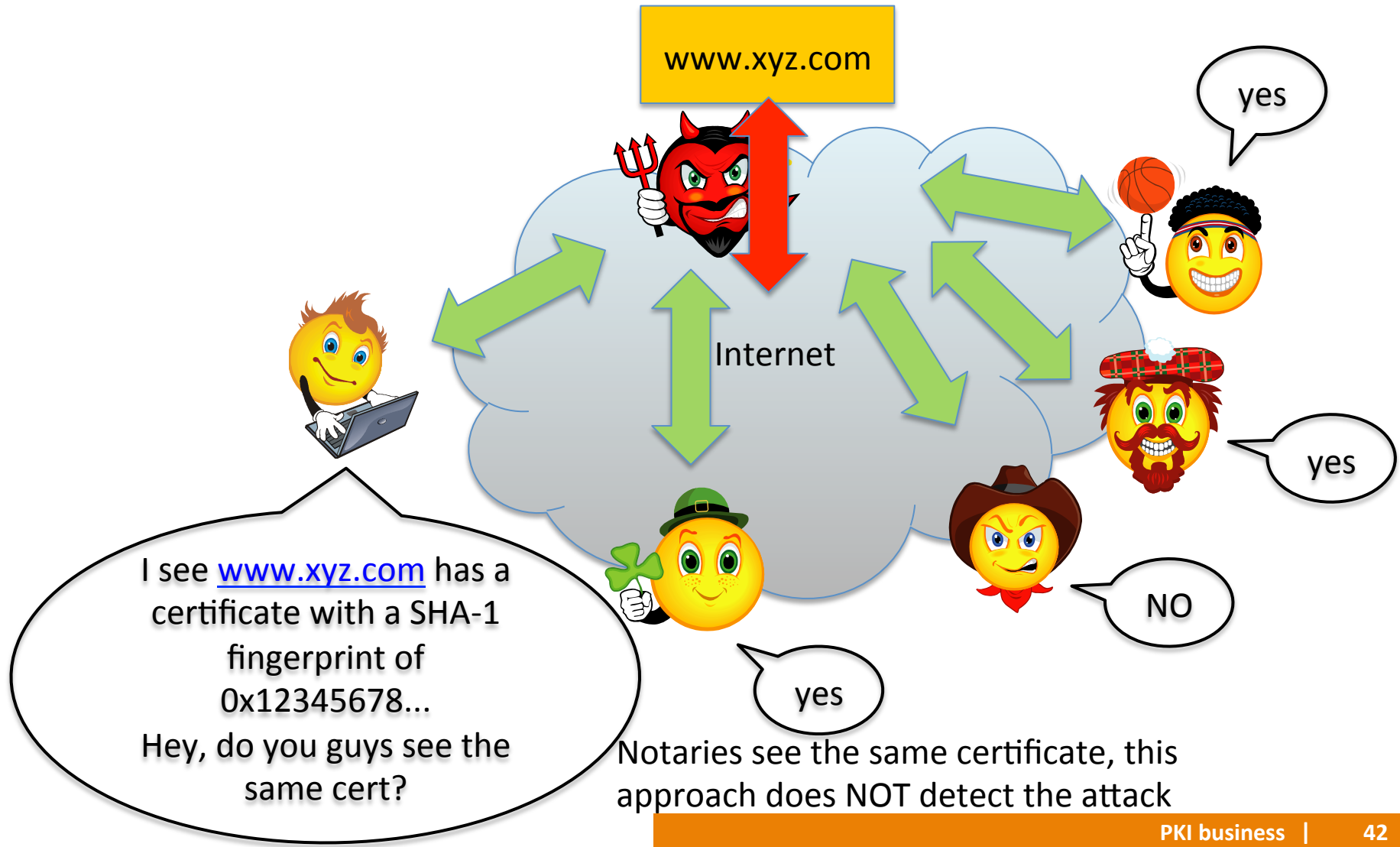
How Perspectives works



Perspectives – Client ISP is Evil



Perspectives – Server ISP is Evil



Notes on TOFU and networked verification

- The Diginotar incident was [detected](#) by a user who saw a different and unknown CA as the issuer of GMail.com
- These approaches struggle if the site's certificate changes quickly legitimately
 - for instance, if a site is supported by multiple servers (for balancing the load) that have different certificates (because each server has a different key pair)

Tool: Convergence

- An extension of Perspectives, by Moxie Marlinspike
- More control over votes from notaries (consensus, majority vote, etc.)
- Uses onion routing for anonymous connections to notaries
- <http://convergence.io/>, [Firefox Addon](#)

Summary of concepts presented

- TOFU & Identity change detection (certificate pinning)
 - provides forward secrecy
 - example: Certificate Patrol
- Networked verification of identity
 - works if the man-in-the-middle attack is targeted at a client, and not at the whole web
 - example: Perspectives, Convergence
- Encrypting / Authenticating the connection based on the key obtained the above way, via regular TLS

Conclusions

- There is no major problem with TLS and web-based PKI
- Of course, you should not trust it blindly, it has limitations
- TLS provides sufficient protection against most attackers, but does not help against those few who can tamper with CAs
- Identity change detection and network verification of identity approach the problem differently, they can be viable
- I do not think any of the presented tools/approaches are significantly better than PKI-based TLS, they are cheaper but (probably) have a lower level of security
- Security geeks can combine these currently immature tools with PKI-based TLS to gain more security