Trust Router Trust Model

David Chadwick
University of Kent

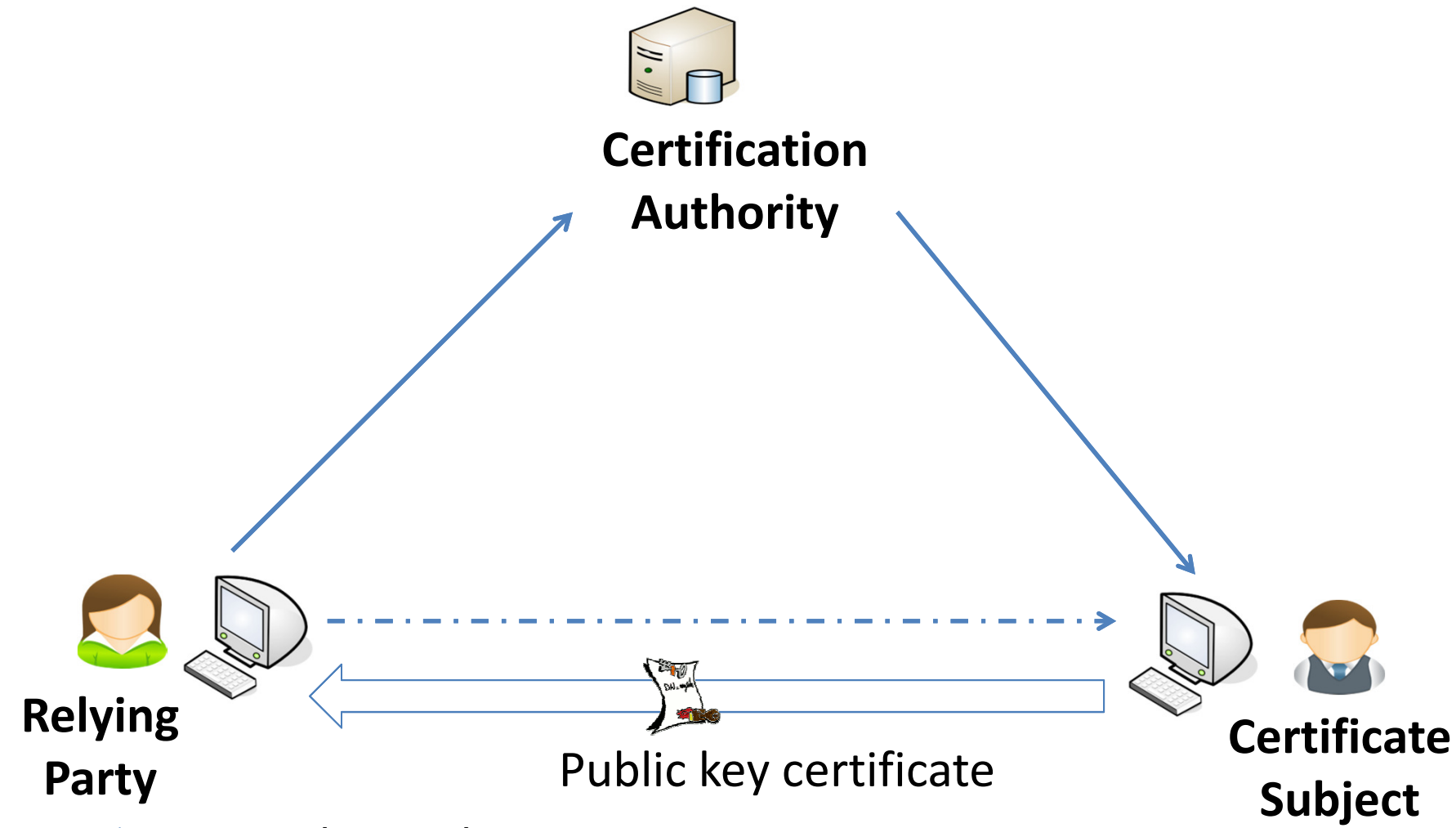
Trust in What?

- A trustor trusts a trustee to perform a certain action as expected
- In the case of the ABFAB Trust Router:
- Trustor -> AAA client of RP
- Trustee -> Trust Routers of an ABFAB infrastructure
- Action -> route temporary identity protocol request to the correct AAA server (that is capable of authenticating users for the identified realm)
- As expected -> to the required level of assurance as described in the ABFAB Infrastructure Participation Policy (or whatever name you want to give it)
  - Note. This is not the APC. The IPP is not concerned with user authn

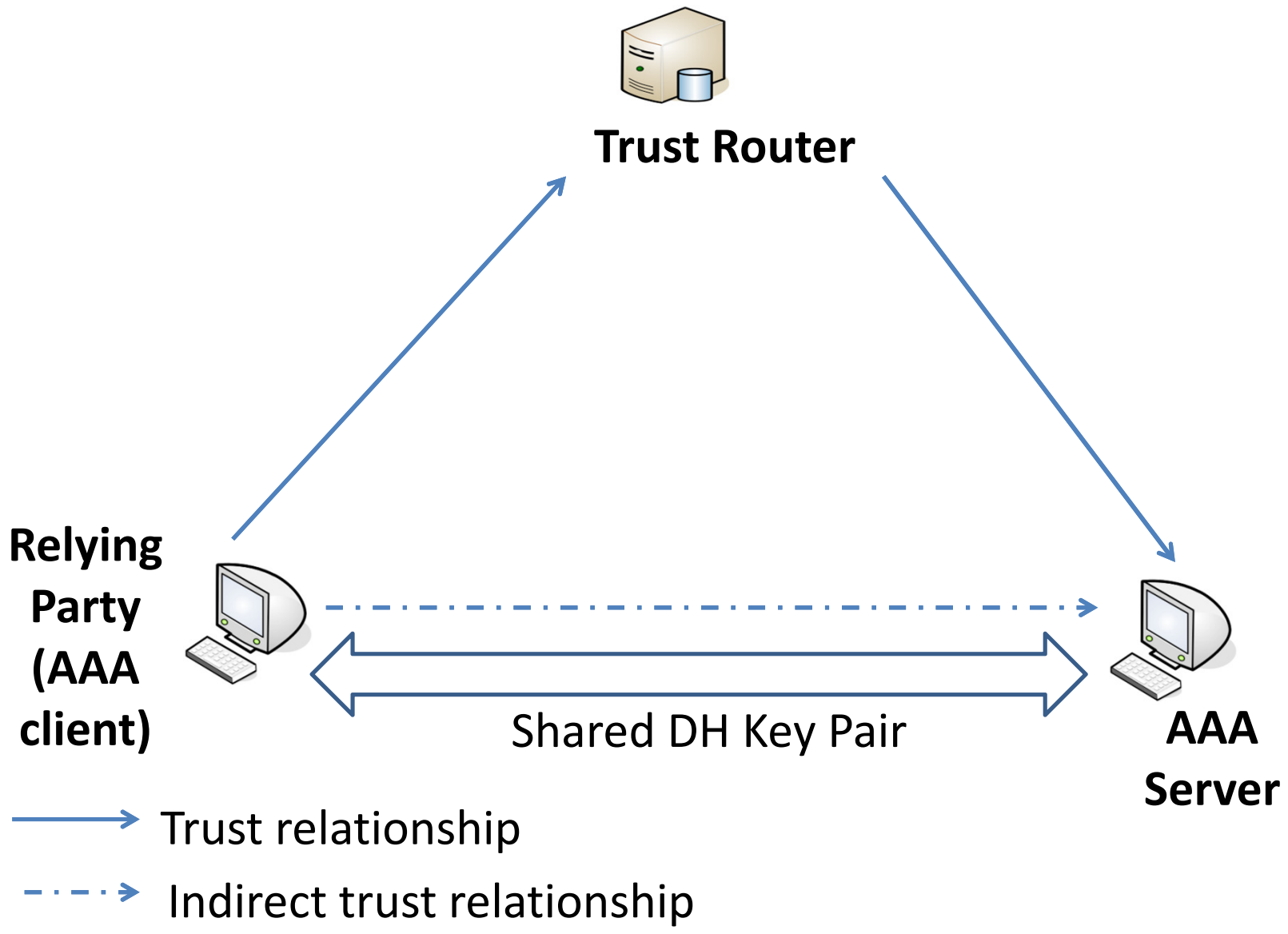
An Analogy

- Compare PKI Infrastructure with Trust Router Infrastructure
- In PKI, the RP trusts the CA (trust anchor) to authenticate subjects
- The CA trusts the certificate subject (having authenticated them)
- Two strangers can authenticate each other based on this
- The RP can indirectly trust that the subject is who he claims to be based on the certificate (subject DN or alternate name) as it was issued by the trusted CA

PKI


Certification Authority
Relying Party
Public key certificate
Certificate Subject
Trust relationship
Indirect trust relationship

ABFAB


Trust Router
Relying Party (AAA client)
Shared DH Key Pair
AAA Server
Trust relationship
Indirect trust relationship

ABFAB Trust in Authentication

- Trust router is responsible for introducing two strangers and sharing a DH key pair between them
- AAA Client trusts the ABFAB Trust Router to route temporary identity protocol request to the correct AAA server (that is capable of authenticating users for the identified realm)
- Trust Router trusts that AAA server is capable of authenticating users for the identified realm, because its administrator has validated this
- AAA Client indirectly trusts (unknown) AAA server it has a shared DH key with to be capable of authenticating users for the identified realm

PKI Analogy Continued

- How do RPs know they can trust the CA in the PKI?
- Because they should check its CP/CPS
- How do RPs know they can trust the Trust Router in the ABFAB infrastructure?
- Because their administrators should check the ABFAB Infrastructure Participation Policy

ABFAB Infrastructure Participation Policy

- Should state the minimal acceptable procedures for how AAA servers and clients for a realm are authenticated and registered with the infrastructure's trust routers
  - Leads to a level of assurance in the ABFAB infrastructure

PKI Analogy Continued

- What if there are multiple trust routers in a given ABFAB infrastructure?
- When one trust router accepts routing information from another trust router, this is equivalent to cross certification between two CAs in a PKI
  - i.e. One party trusts the other. It does not need to be mutual/reciprocal, but it aids routing if it is
- A CA should only cross certify another CA if its CP/CPS is the same as, equivalent to (or better) than its own
  - Otherwise the cross certifying CA needs to start inserting policies into its cross certificates to limit trust, and the whole PKI chain validation starts to get very messy
- Consequently it is preferable if the trust routers have the same Infrastructure Participation Policy
  - Easy to achieve in a single ABFAB infrastructure where all trust routers are in same trust domain
  - More difficult when two different ABFAB infrastructures join together. They need to have equivalent Infrastructure Participation Policies

What Delimits an ABFAB Infrastructure?

- Which realms are members of an ABFAB infrastructure and which are not?
  - Realms that agree to abide by the terms and conditions of the ABFAB Infrastructure Participation Policy are entitled to join
  - A trust router's administrator still needs to invite them, vet them and register them. Probably will involve signing a contract
- Which trust routers are members of an ABFAB infrastructure?
  - Trust router administrators autonomously decide when to join an ABFAB infrastructure and when not to. ABFAB infrastructures can dynamically expand (and contract) – just like EduRoam
- How many ABFAB infrastructures can/should there be?
  - As many as you want, but the fewer the better as they partition the Internet into ABFAB trust domains (how many EduRoams should there be?)
- What should we call one of these ABFAB infrastructures? How about
  - ABFAB Infrastructure Trust Domain
  - Trusted ABFAB Infrastructure ??? Open for discussion

How does an ABFAB Infrastructure Relate to APCs and CoIs?

- APCs and CoIs build on top of an ABFAB infrastructure
- An ABFAB infrastructure can have multiple APCs
- The level of assurance one can assign to an APC is at most equal to the level of assurance in the ABFAB infrastructure
  - You cannot have greater assurance in the authenticity of a user than you can have in the ABFAB infrastructure, since the latter routes user authentication requests from the RP to the AAA server
- An APC could span multiple ABFAB infrastructures, but because their assurance levels are likely to be different, then the APC's LoA would be the lowest of the infrastructure assurance levels
- A CoI can span multiple APCs, but its guaranteed authentication LoA would be the lowest of all the spanned APCs

Implications for Trust Router Protocol

- Each trust router in an ABFAB infrastructure is equally trustworthy
  - They all conform to the same ABFAB Infrastructure Participation Policy
  - Thus a trust router cannot decide that some routing info it receives from another trust router is trusted and some is not as this breaks the trust model
- Propagating routing and CoI information within an ABFAB infrastructure could be ad hoc
  - Each trust router decides who to propagate information to in an ad hoc manner
- Or it could be managed
  - E.g. have master/slave trust routers and peer trust routers and a defined procedure, as per the Internet Draft “A Trust Model for ABFAB Trust Routers” <draft-dwc-abfab-trust-model-00.txt>. NB. This ID needs updating

Some Final Thoughts

- If ABFAB becomes as successful as PKI, you could have many hundreds of trust routers in many different ABFAB trust domains, with millions of AAA servers linked to them
  - And chaos for users and RPs who wish to authenticate each other
- You could have a global CA web of trust where different CAs cross certify other CAs to different levels of assurance, but this would lead to multiple levels of trust and complexity when trying to validate certificate chains
  - Similarly we don't want trust routers interconnecting together in a web like manner using different Infrastructure Participation Policies. Trying to work out the trustworthiness of this mesh would be next to impossible