Trust Management in PKI

Priyadarshi
Research Scholar

University of Hyderabad

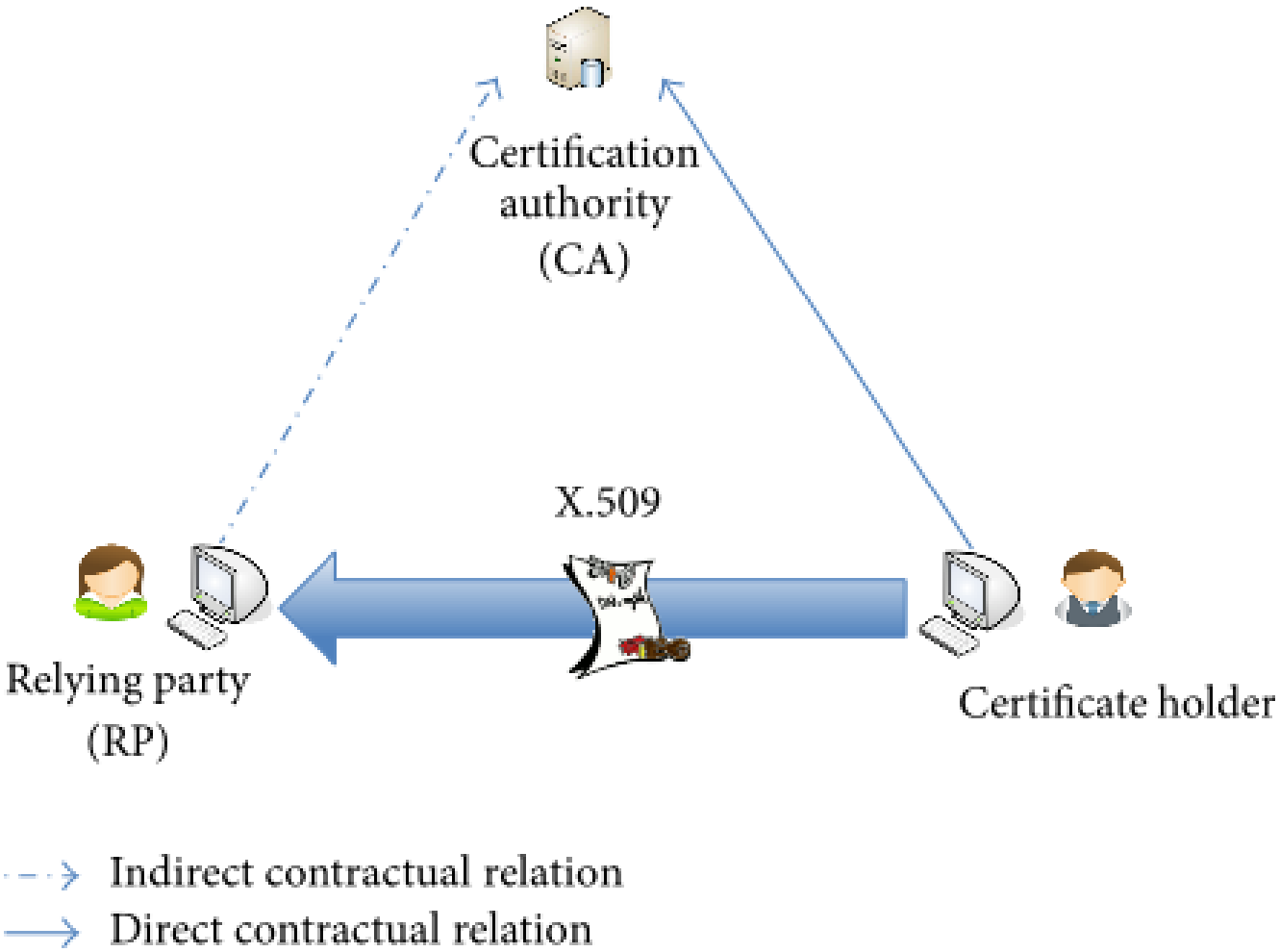
priyadarshi.024@gmail.com

November 14, 2017

About the Talk

- Concerns about the deployment Issues of PKI
- Assessing the Trustworthiness of CA
- A Better Trust Management
- Research Challenges

X.509 Trust Model



Motivation for Talk

- Why RP should "TRUST" CA?
- Computational Trust in PKI

Problems persisting in present PKI implementations:

- Computers don't understand the semantics of a policy
- Cross Certification requires equal policies
- PKIs don't handle trust dilution
- PKIs don't take into account parallel certification paths
- PKIs give little support for decision making

Trust Management in PKI

- Trust management includes methods for assessing policies regarding issuance and handling of public-key certificates and for determining whether these policies are adhered to by CAs and users, with the purpose of making decisions
- Trust Assessment must be based on some initial trust combined with trust propagating mechanisms, and should provide a basis for decision making

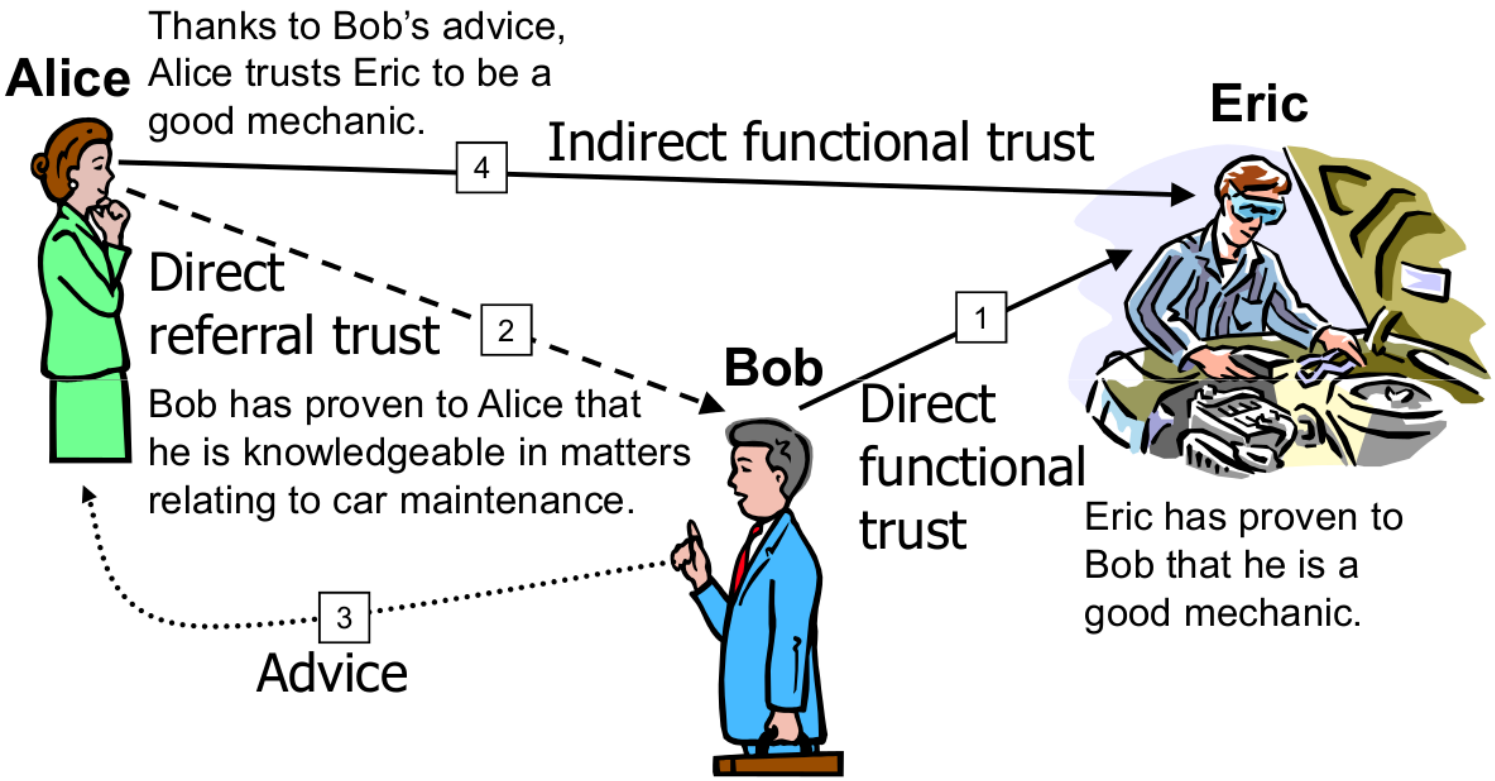
Two Definitions of Trust:

- Belief Trust: The Subjective beleif by which an indiviadual, A, thinks that another entity B ,performs a given action on which A's welfare depends (Gambetta 1998)
- Decision Trust: The decision to depend on something or somebody in a given situation with a feeling of relativity, even though negative consequences are possible (Mcknight & Chervang 1996)

Some Trust Semantics

- Trust Scope: The combined set of functions that the relying party depends on & trusts
- Functional Trust: The trusted party actually performs the functions of the trust scope
- Referral Trust: The trusted party recommends a party that can perform the functions of the trust scope.

Trust Transitivity



Computational Trust in PKI

- Trust Modelling
- Subjective Logic Based Trust Networks
- Computing Trust in PKI

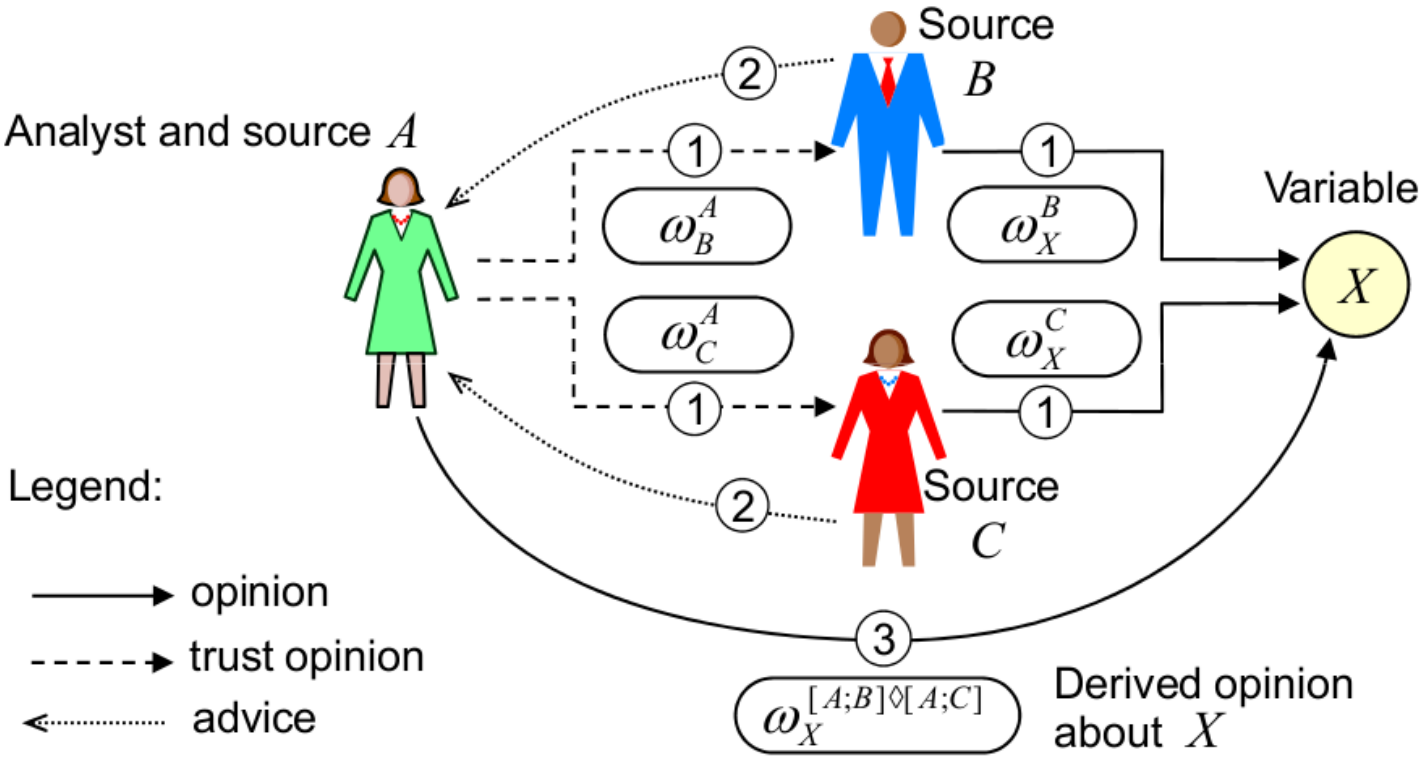
Subjective Logic

- Formalized by Prof. Audung Josang
- It is a type of probabilistic logic that explicilty takes uncertainity & belief ownership into account
- Suitable for modeling and analysing situation involving uncertainity & incomplete knowledge

e.g Modeling Trust Networks, Analysing Bayesian Networks.

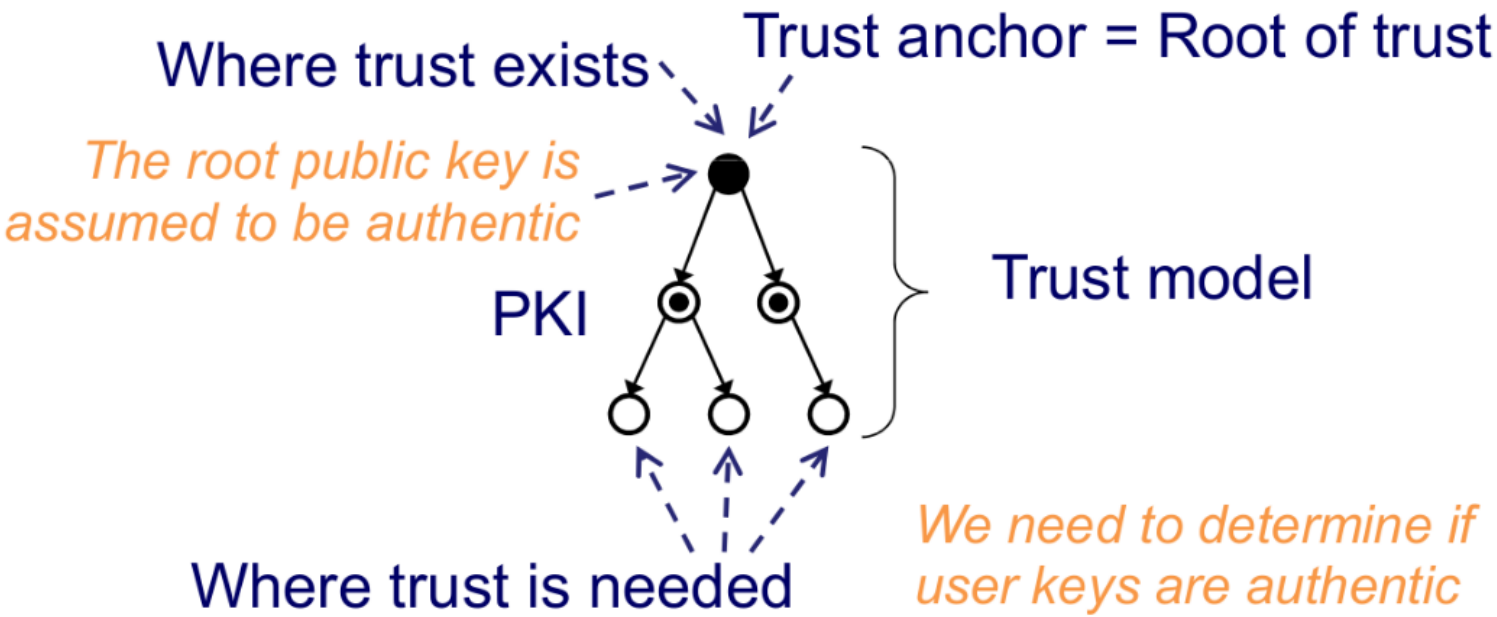
Subjective Trust Networks

Trust Network based on Subjective Logic can be modelled with a combination of the transitivity/ discounting & fusion operator.

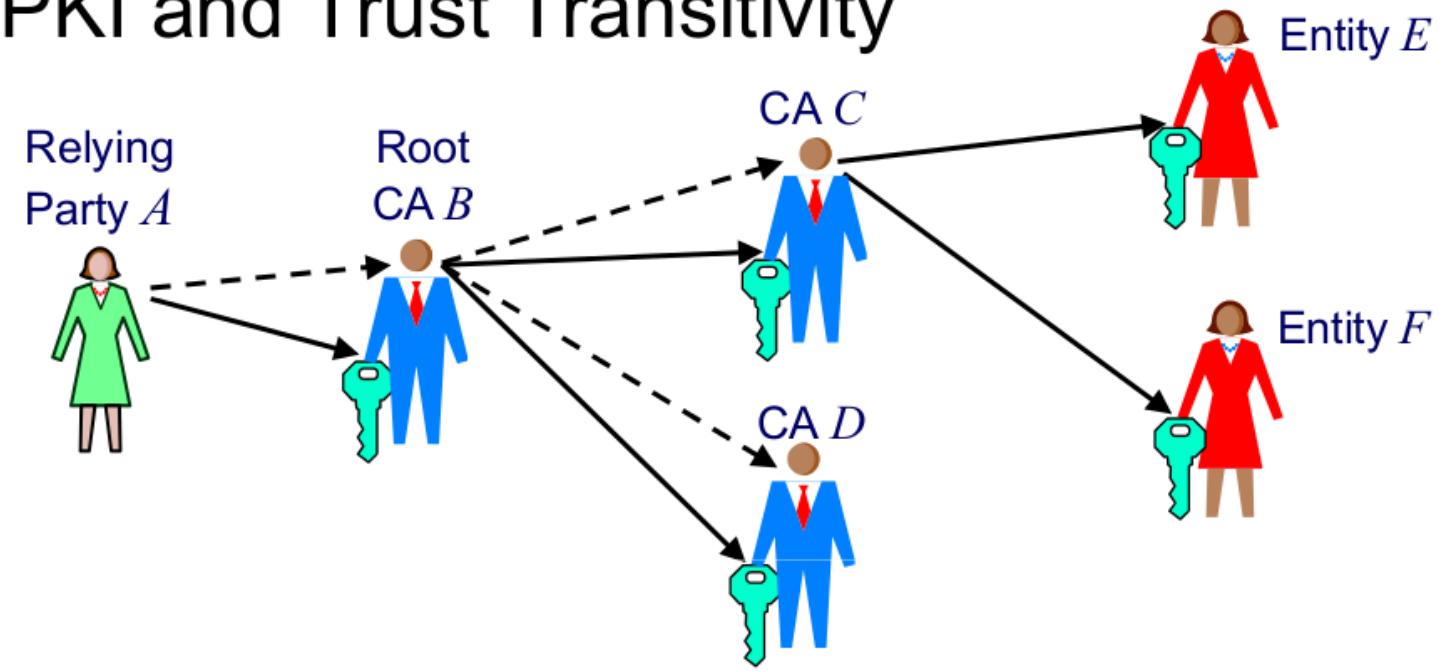


Propagation of Trust

- A PKI allows to be propagated from where it exists to where it is needed (Simmons and Meadows,1995)



PKI and Trust Transitivity



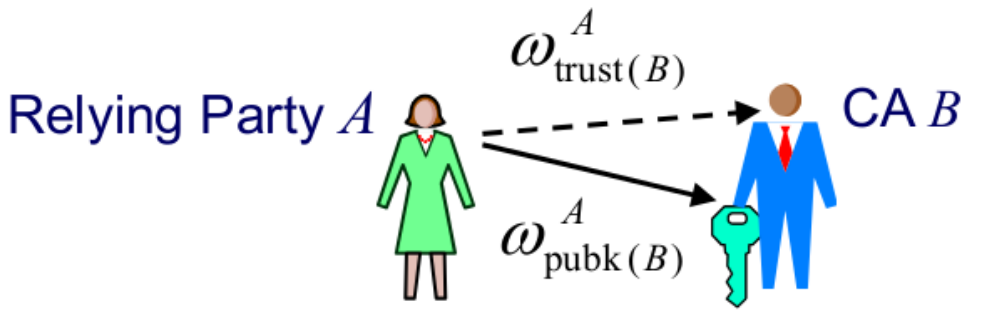
Functional trust in the public key

(I have the CA/entity's authentic and uncompromised public key)

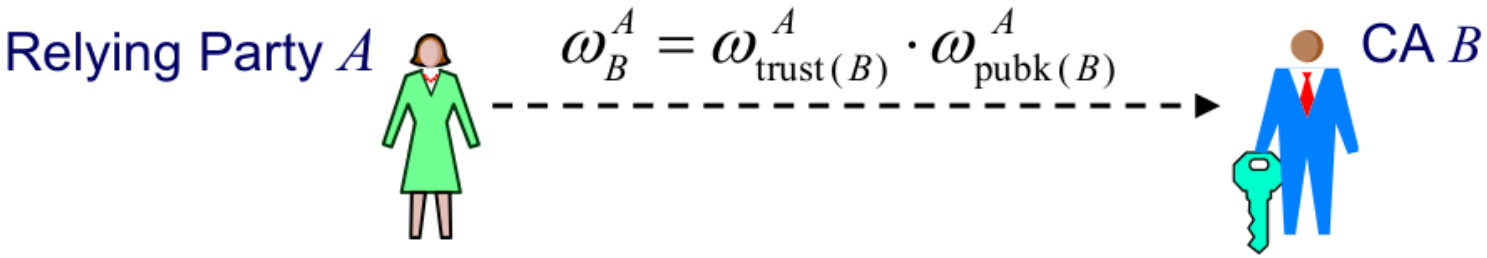
Referral trust in the CA

(I trust the CA to issue correct public-key certificates)

Computing Trust in PKI Certificates



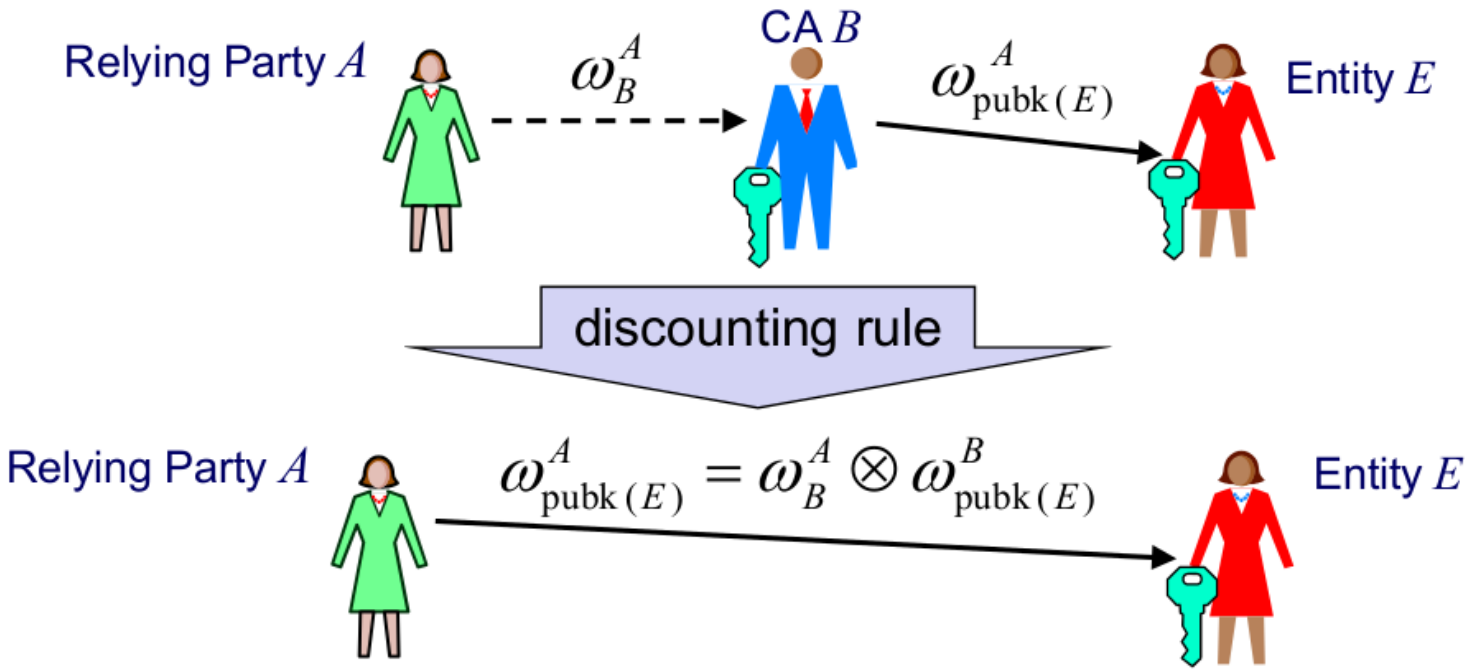
Product rule



Note that ω^{A}_{B} can also be denoted as $\omega^{A}_{\text{trust}(B)\times\text{pubk}(B)}$

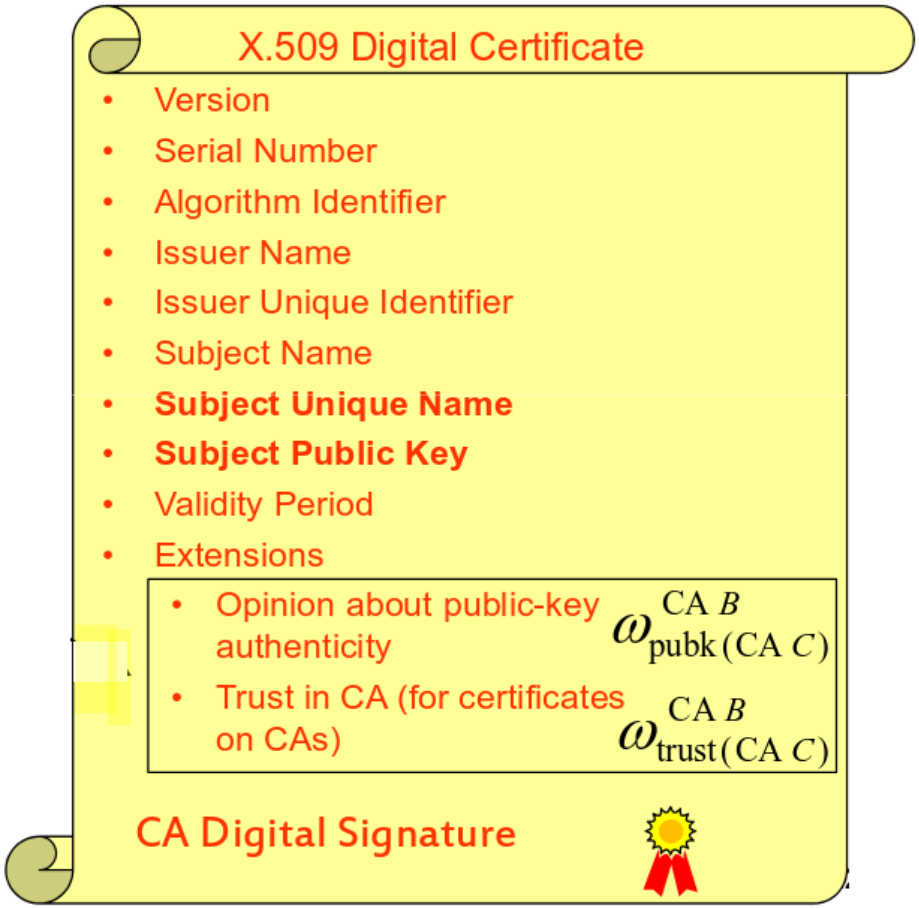
ω^{A}_{B} expresses A's trust in certificates signed by B's public key

PKI and Trust Transitivity

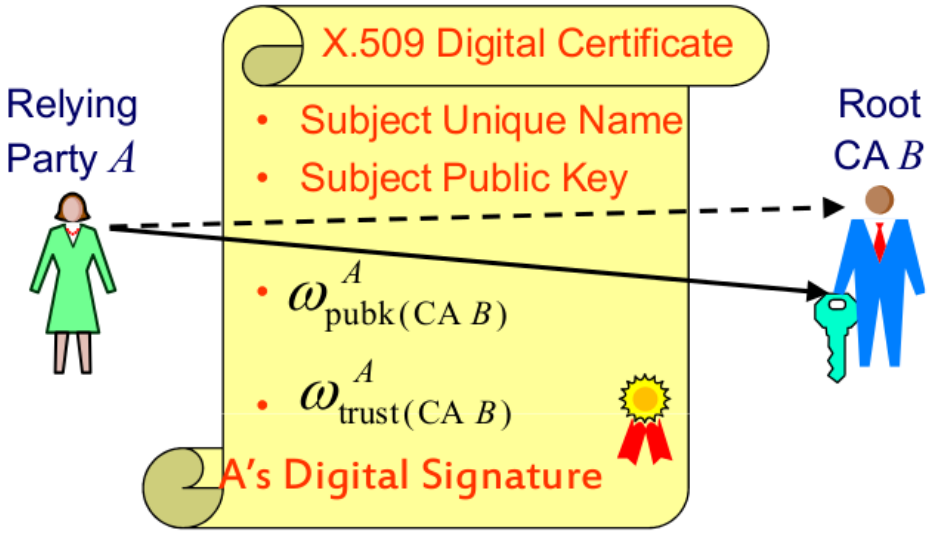


$\omega_{\text{pubk}(E)}^A$ expresses A's belief in the authenticity of E's public key

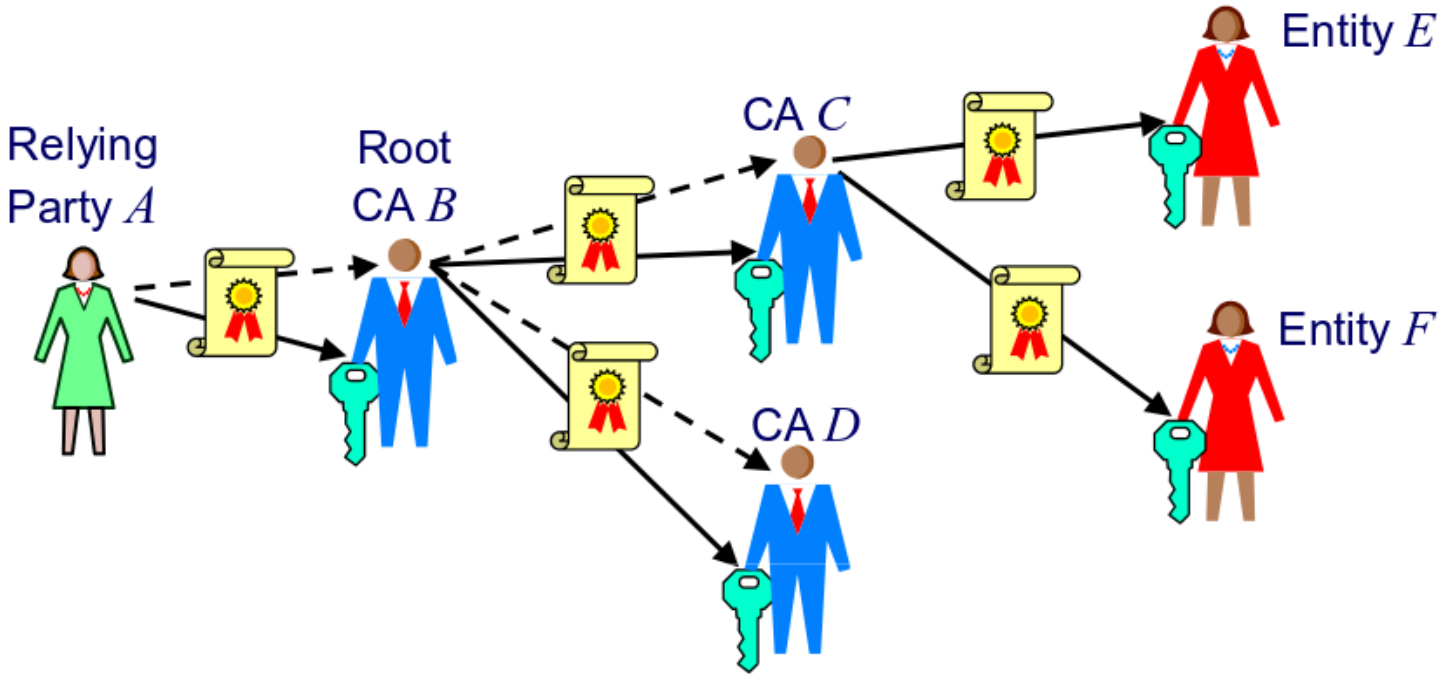
Trust Extensions in X.509 Certificates



Root Certificate Signed by Relying Party



- The PKI Trust model assumes that relying party generates self-signed certificates for the root CAs.
- Certification by relying parties transforms traditional PKIs into user-centric PKIs similarly to the PGP PKI.



- A's derived opinion about the authenticity of E's public key can be computed as:

$$\omega^{A}_{\text{pubk}(E)} = \omega^{A}_{B} \otimes \omega^{B}_{C} \otimes \omega^{C}_{\text{pubk}(E)}$$

Research Challenges

- Reliable Trust Evaluation methods for closed deployment PKI
- Interoperability Issue of open deployment PKI

References

- "PKI seeks a Trusting Relationship", by Audun Josang
- ITU. Recommendation X.509, The Directory Authentication Framework, ITU-T 1993
- Subjective Logic, A formalism for reasong under uncertainty, springer 2016, Audun Josang
- Trust Management for Public Key Infrastructures: Implementing the X.509 Trust Broker, Chadwick et al, 2017

THANKS FOR LISTENING !!