Course: Modern Cryptography

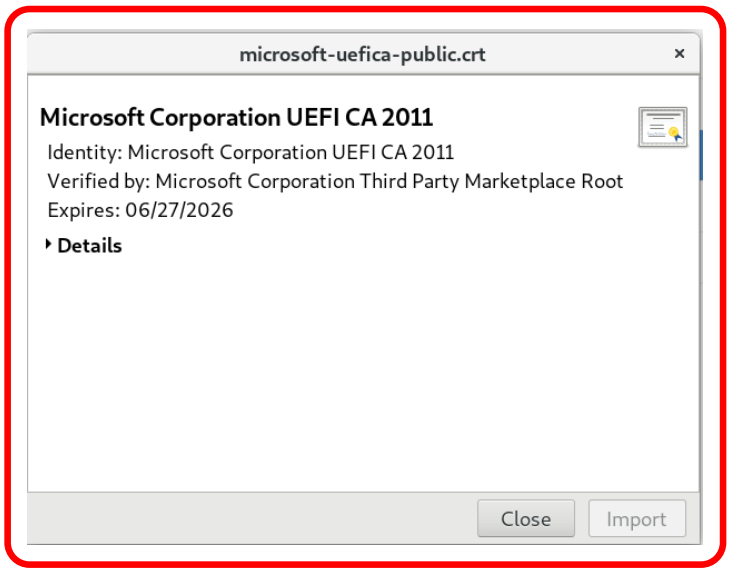
Certificates and Public-Key Infrastructures

Shashank Singh

IISER Bhopal

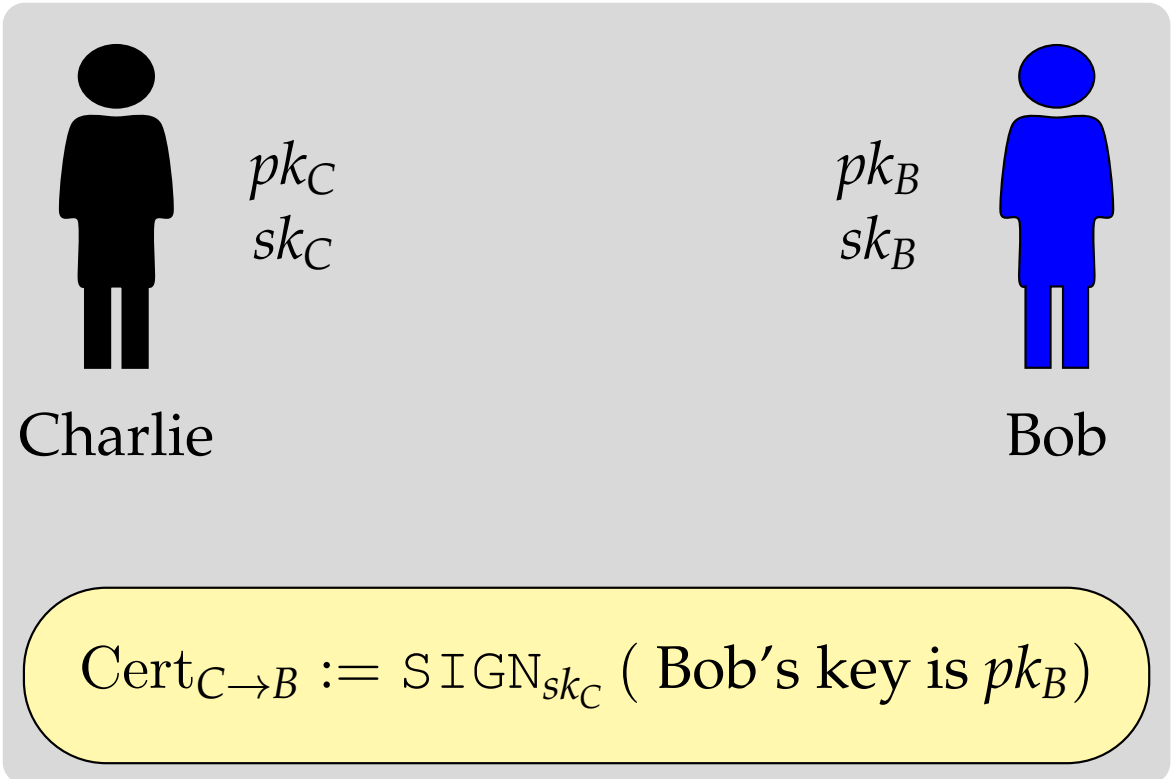
November 12, 2025

Digital Certificate



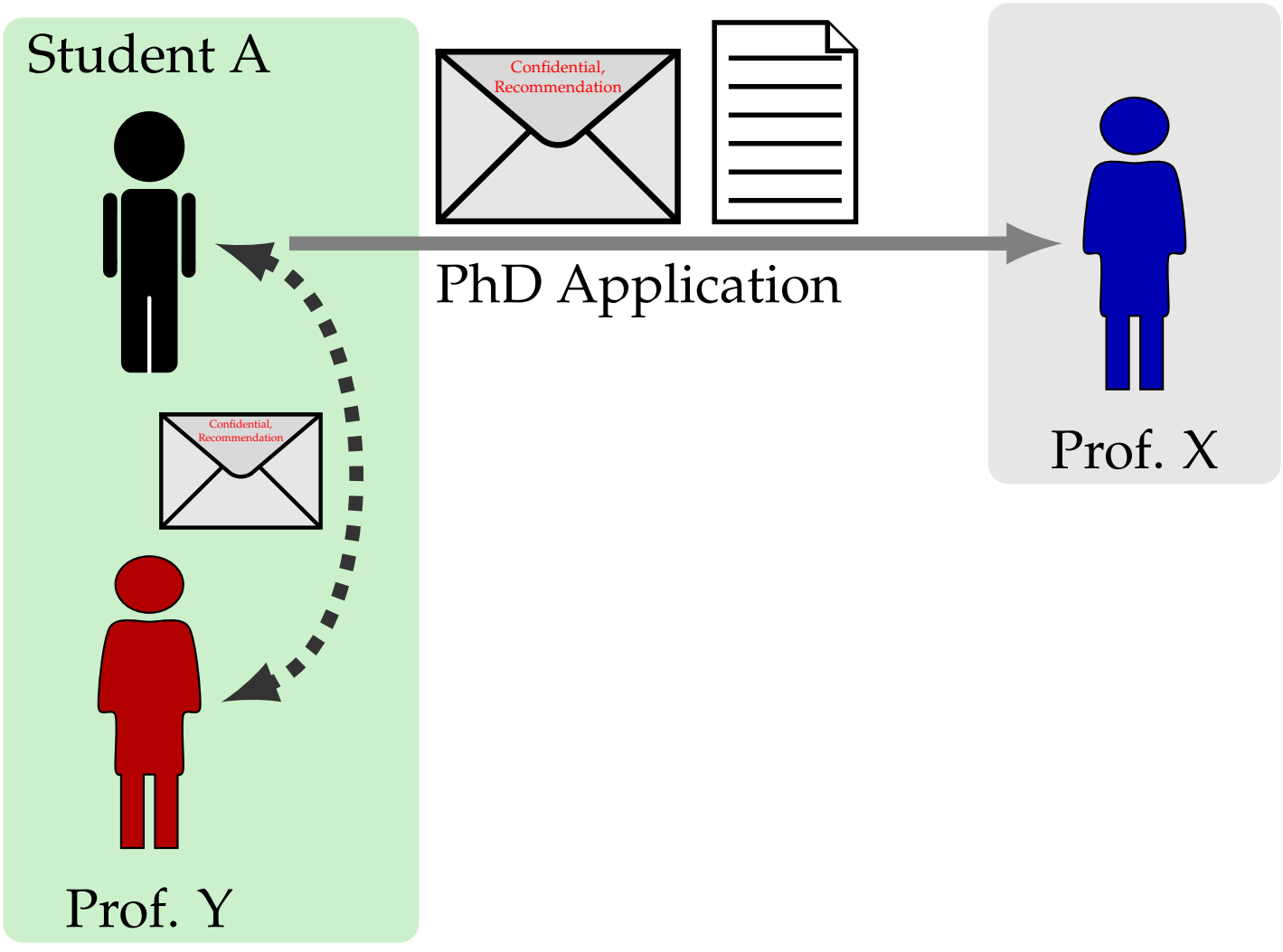
- It is used to link ownership of a public key with the entity that owns it.
- It includes the public key, owner information, metadata and a digital signature of the public key created by the issuer.

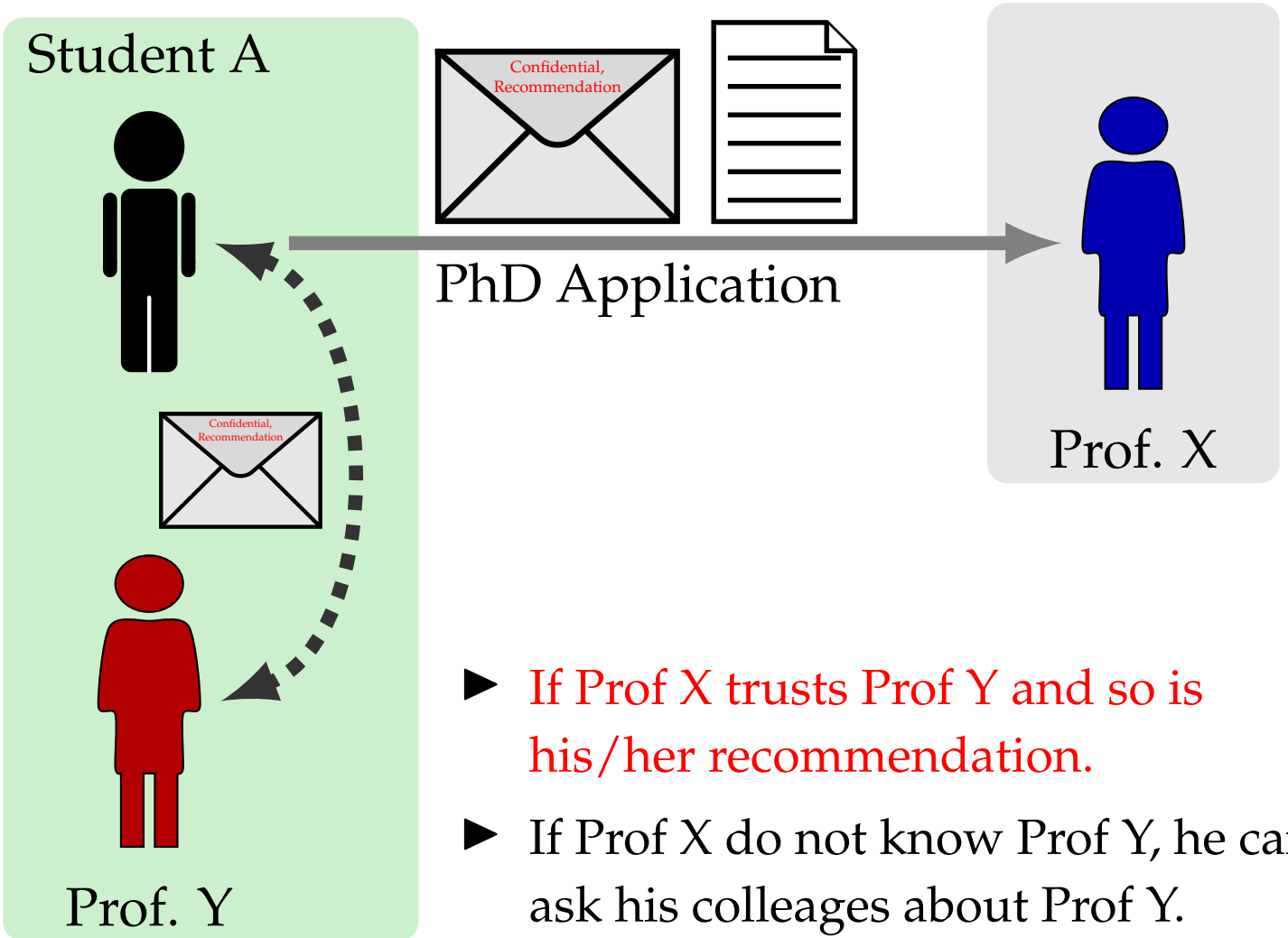
A digital certificate is, in fact, a digital signature of a "public key and its owner information".



- We call $\mathrm{Cert}_{C\to B}$ a certificate for Bob's key issued by Charlie.

- Now say Bob wants to communicate with some other party Alice who already knows the authentic copy of pk_C.
- Bob can send $(pk_B, \mathrm{Cert}_{C \to B})$ to Alice, who can verify $\mathrm{Cert}_{C \to B}$ and if Alice trusts Charlie, she can accept pk_B as Bob's legitimate public key.
- The communications can be done over any public channel without any security issue.


Student A
Confidential,
Recommendation
PhD Application
Prof. X
Confidential,
Recommendation
Prof. Y



- If Prof X trusts Prof Y and so is his/her recommendation.
- If Prof X do not know Prof Y, he can ask his colleages about Prof Y.

Public-key Infrastructure (PKI)

- It is a system that enables the safe/secure distribution of public keys.
- A variety of different PKI models have been suggested. We provide a very high level description of a few of them only.

A Single Certificate Authority PKI Model

- This model assumes a single certificate authority (CA) who is completely trusted by everybody and it is the CA who issues certificates for everyone's public key.
- A certificate authority (CA) is typically a company whose business it is to certify public keys.
- The public key of CA must be distributed over an authenticated channel to users. In practice the pk_{CA} comes bundled with popular software applications.

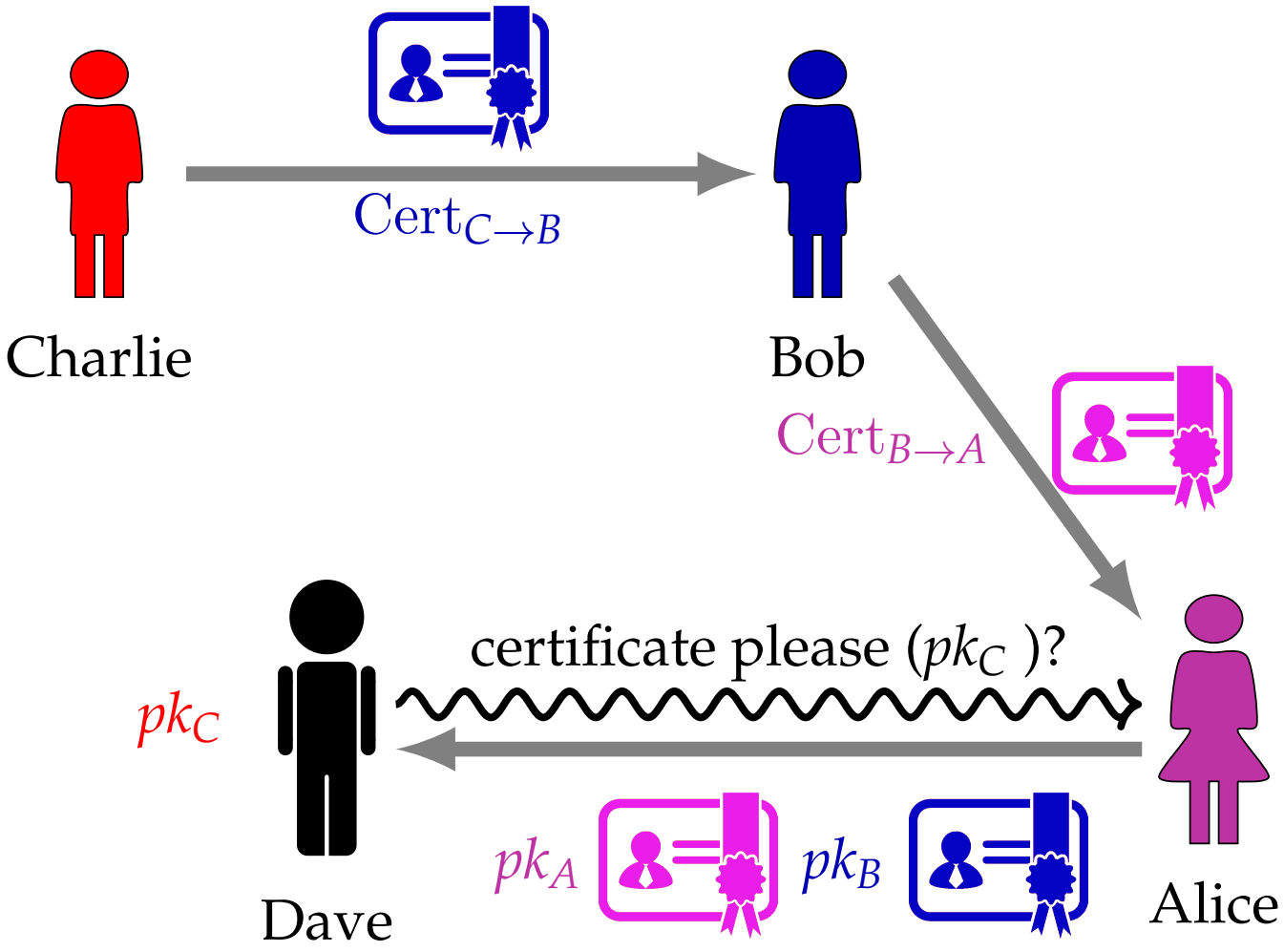
A Single Certificate Authority PKI Model..

- For getting a certifcate, a user may have to show up in person with a copy of his public key along with identification proving that his name (or his email address) is what he claims. A certificate is issued upon successful verification of all the required details.

Multiple CAs PKI Model

- As the name indicates, this model assumes multiple CAs. It is more practical model than single CA model.
- A party Bob who wants to obtain a certificate on his public key can choose which CA(s) it wants to issue a certificate.
- A party Alice who is presented with a certificate, or even multiple certificates issued by different CAs, can choose which CA's certificates she trusts.
- The rest of things are similar to that of single CA model i.e., the public keys of CAs need to be distributed over autheticated channel and a user requesting for certificate needs to present valid documents etc..

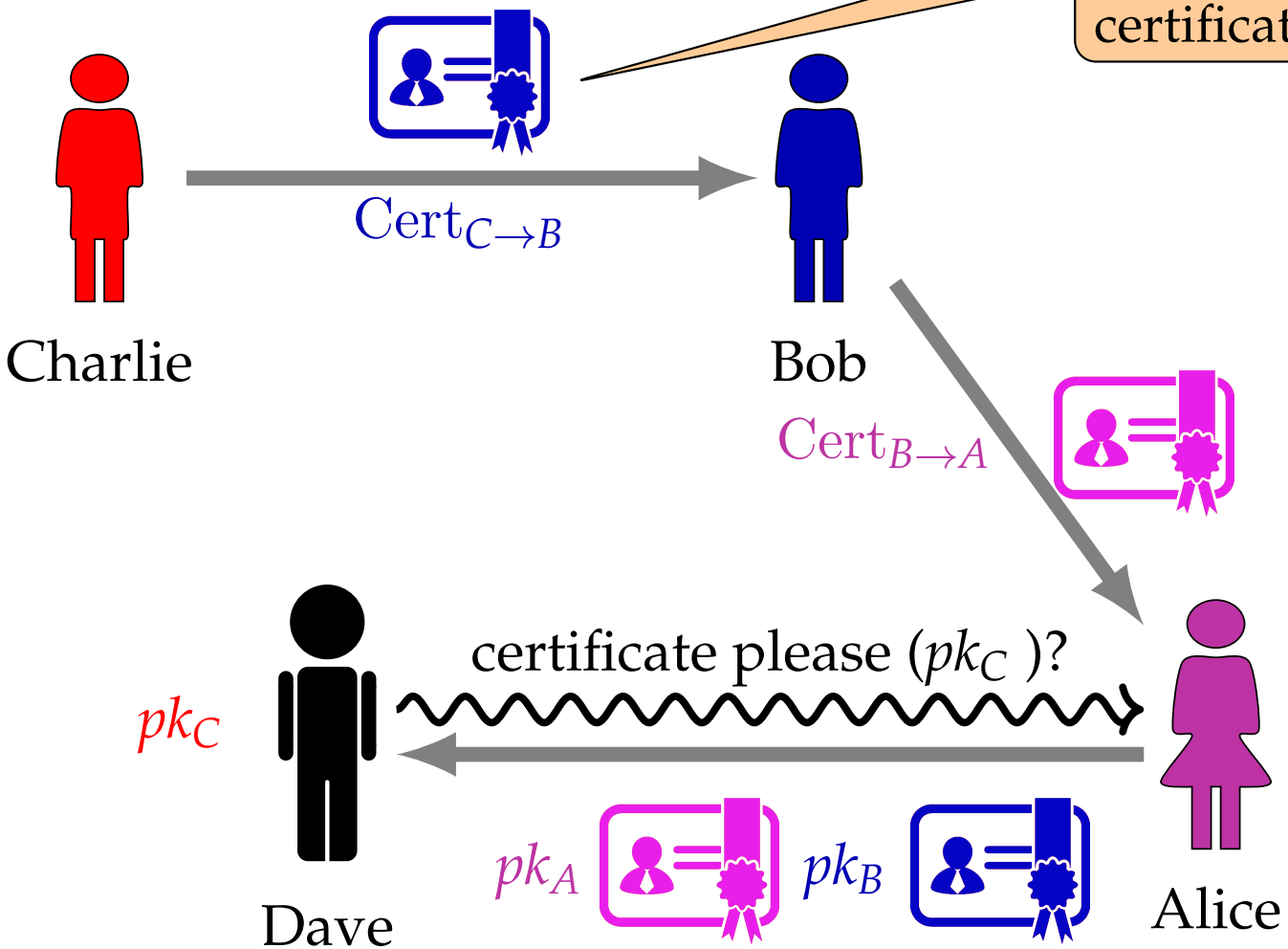
Delegation and certificate chains



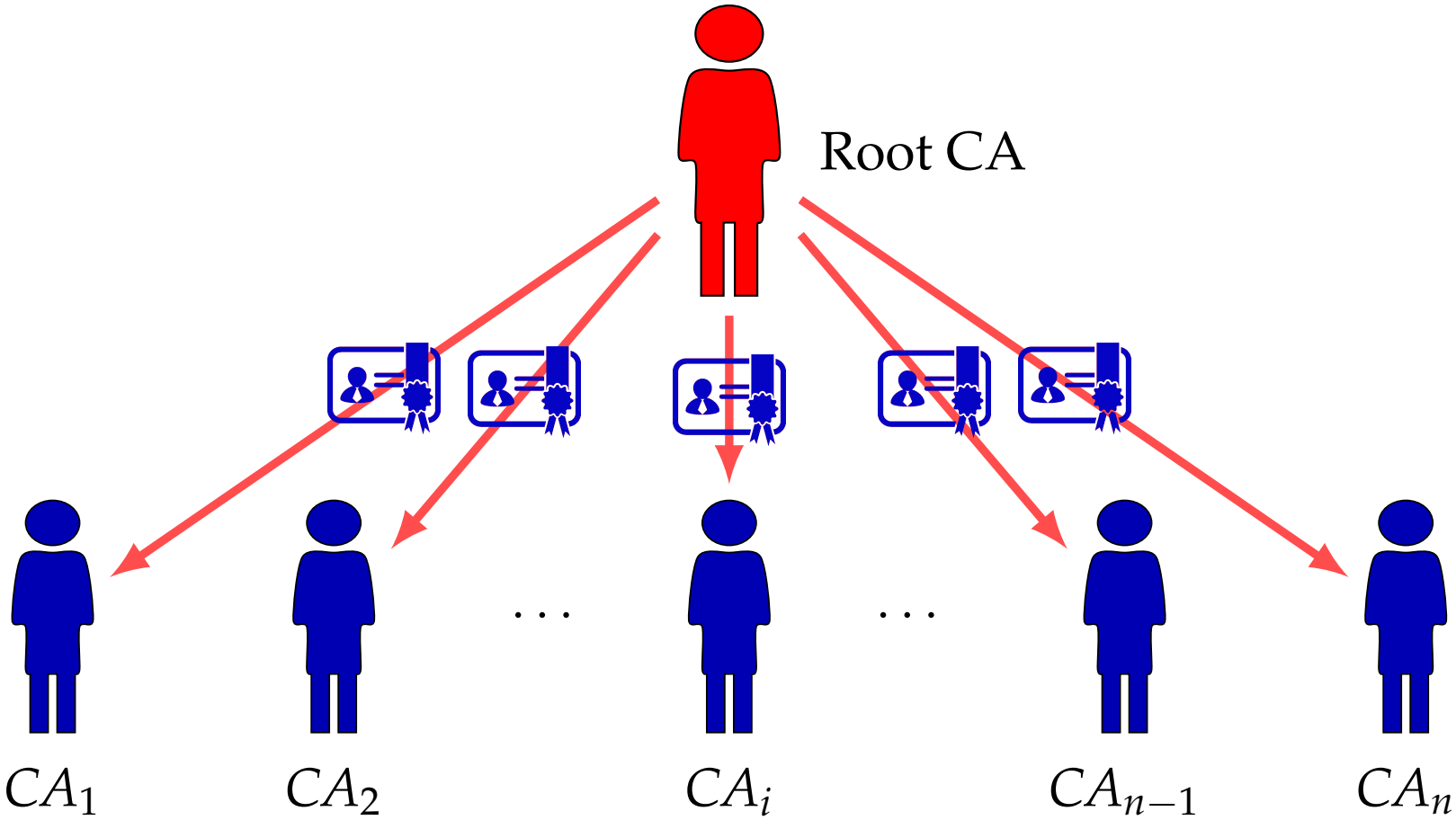
Delegation and certificate ch

Stronger semantics:

It asserts that Bob holds public key pk_B and Bob is trusted to issue other certificates.

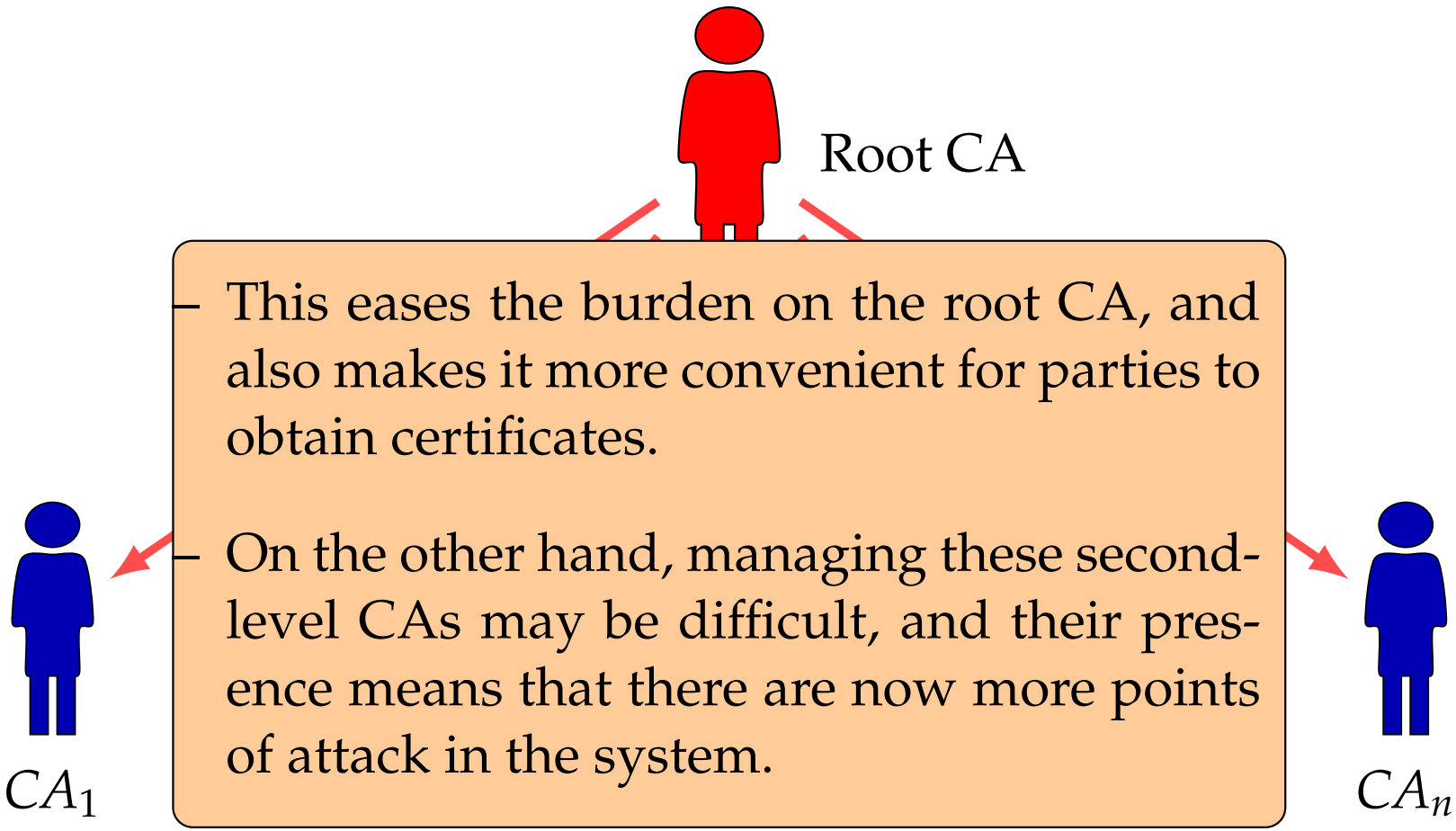


Hierarchy of CAs in CA-based PKI



– The root CA can issue certificates for each of the second-level CAs, who can then in turn issue certificates for other principles holding public keys.

Hierarchy of CAs in CA-based PKI



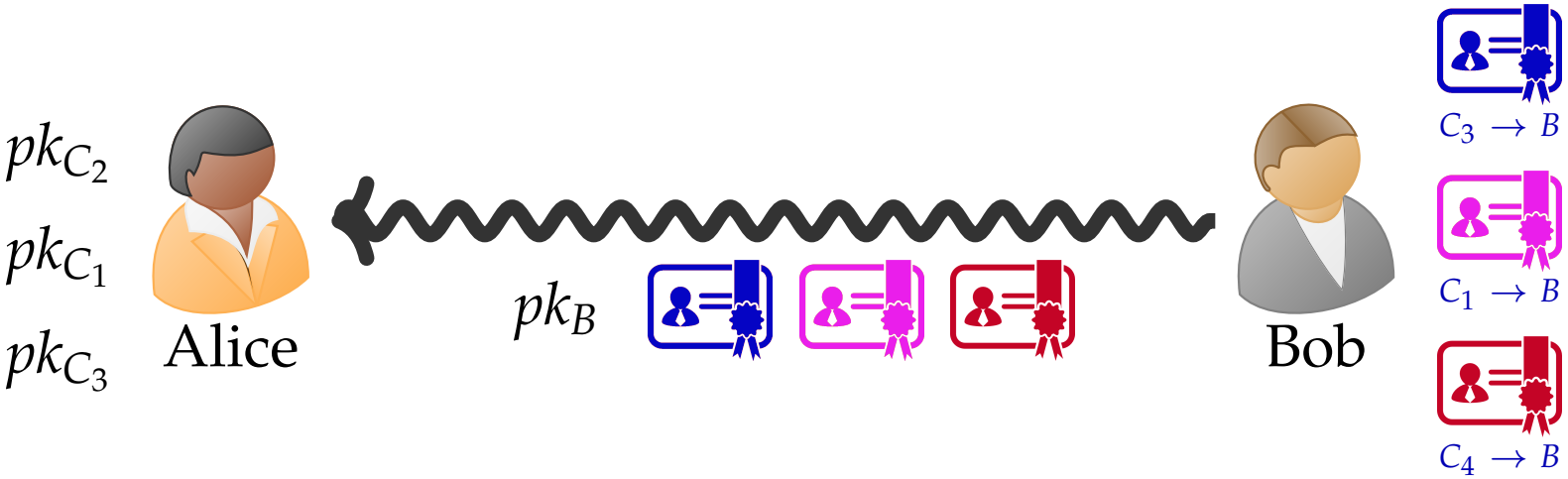
- This eases the burden on the root CA, and also makes it more convenient for parties to obtain certificates.
- On the other hand, managing these second-level CAs may be difficult, and their presence means that there are now more points of attack in the system.

- The root CA can issue certificates for each of the second-level CAs, who can then in turn issue certificates for other principles holding public keys.

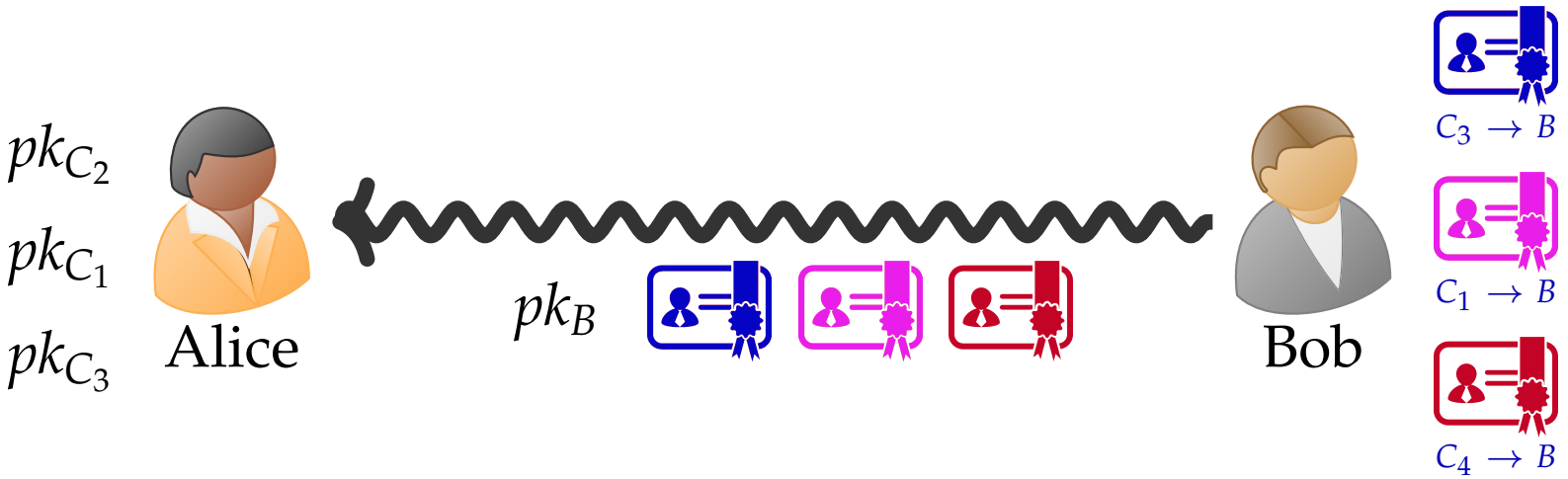
The "web of trust" Model of PKI

- It is a fully distributed model, with no central points of trust.
- Anyone can issue certificates to anyone else and each user has to make their own decision about how much trust to place in certificates issued by other users.

The "web of trust" Model of PKI..



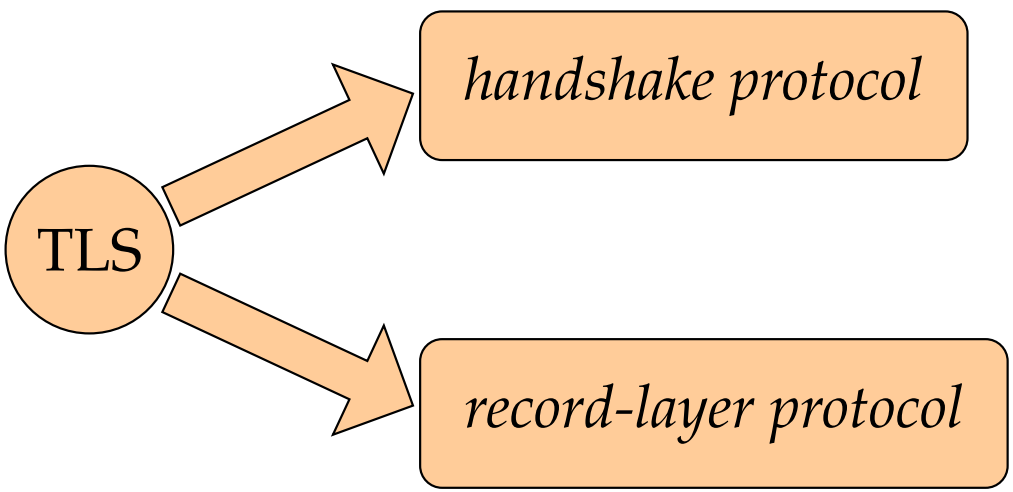
THE "WEB OF TRUST" MODEL OF PKI..



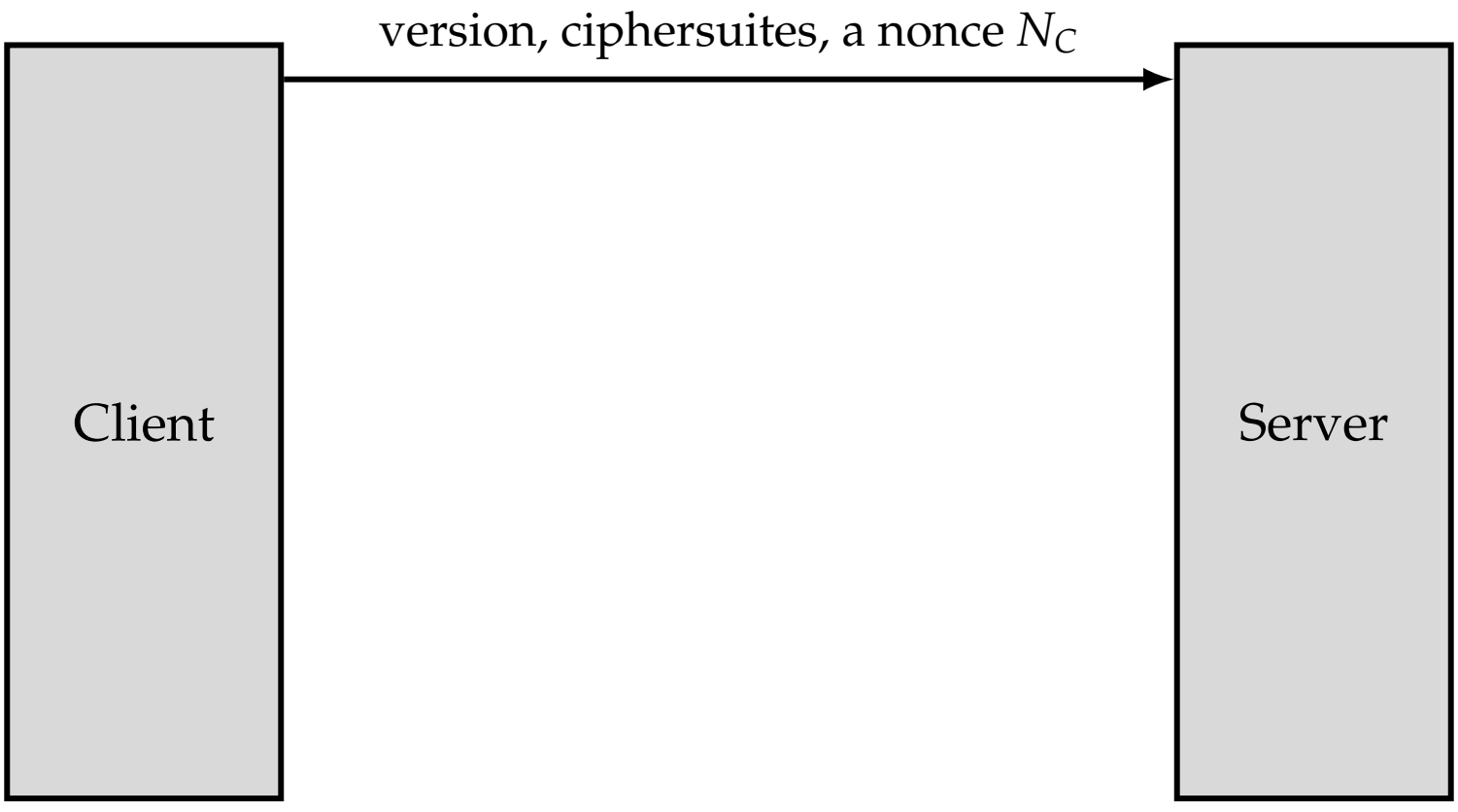
- A user Alice has authentic copies of public keys pk_{C_1}, pk_{C_2}, pk_{C_3} corresponding to users C_1, C_2, C_3.
- Another user Bob who wants to communicate with Alice might have certificates cert $\mathrm{Cert}_{C_1 \to B}$, $\mathrm{Cert}_{C_3 \to B}$, and $\mathrm{Cert}_{C_4 \to B}$, and will send these certificates to Alice.
- Alice can verify the two certificates.
- Alice needs to decide how much trust to place in any of these public keys before using them and depending on it the communication begins.

TLS

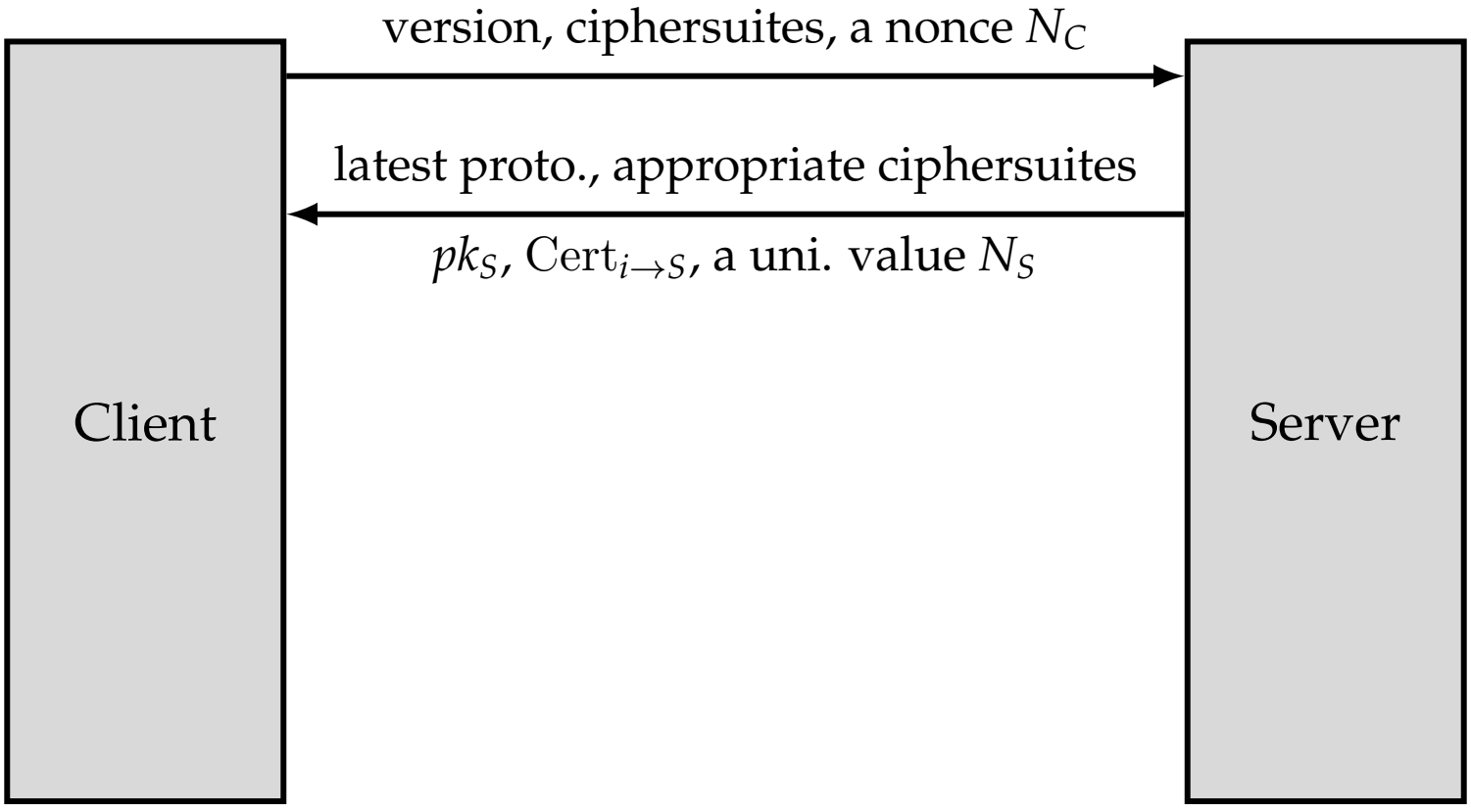
- TLS is the protocol used by your browser any time you connect to a website using `https` rather than `http`.
- TLS allows a client (e.g., a web browser) and a server (e.g., a website) to agree on a set of shared keys and then to use those keys to encrypt and authenticate their subsequent communication.
- TLS has two parts.



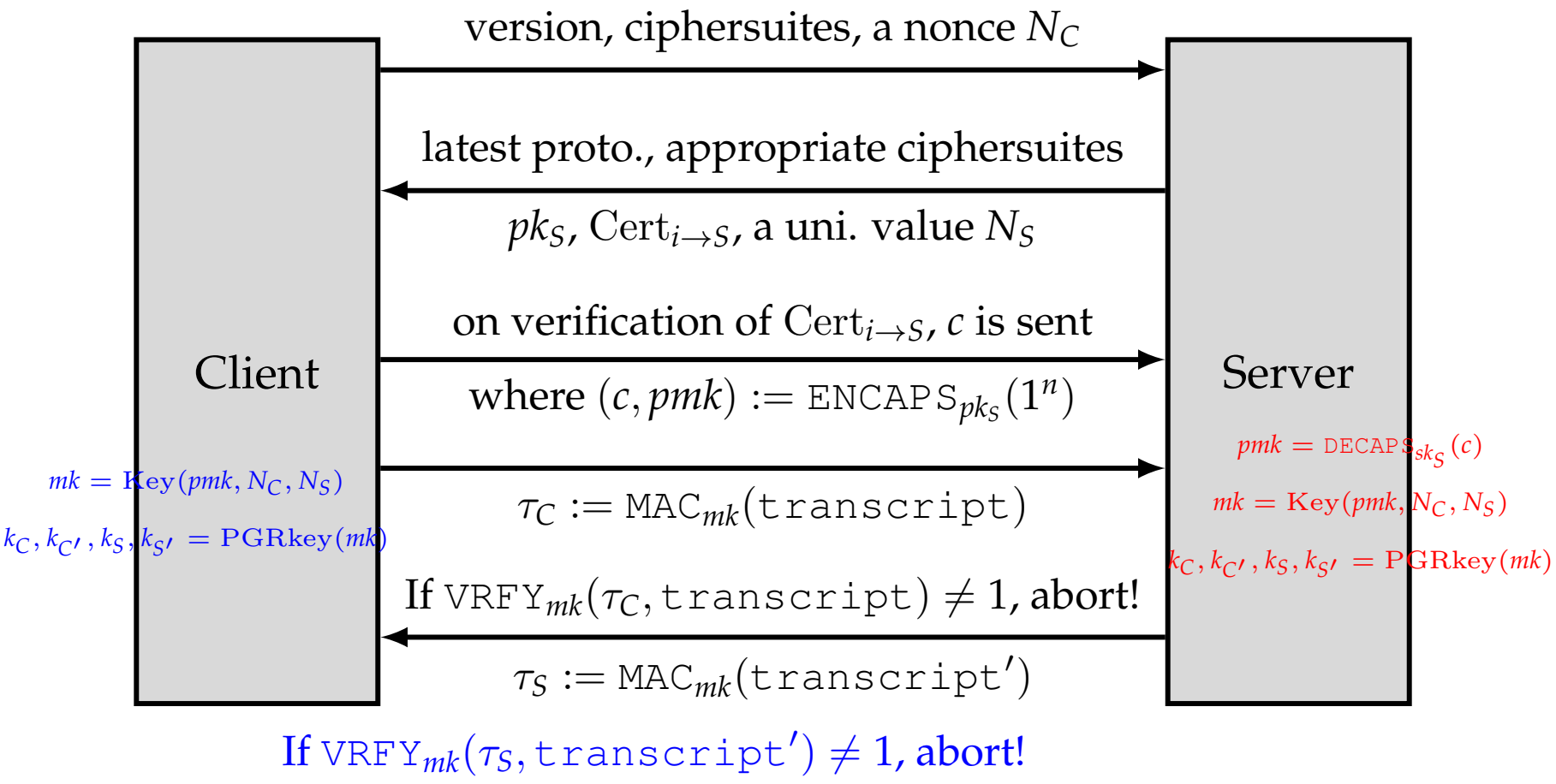
Handshake Protocol



Handshake Protocol

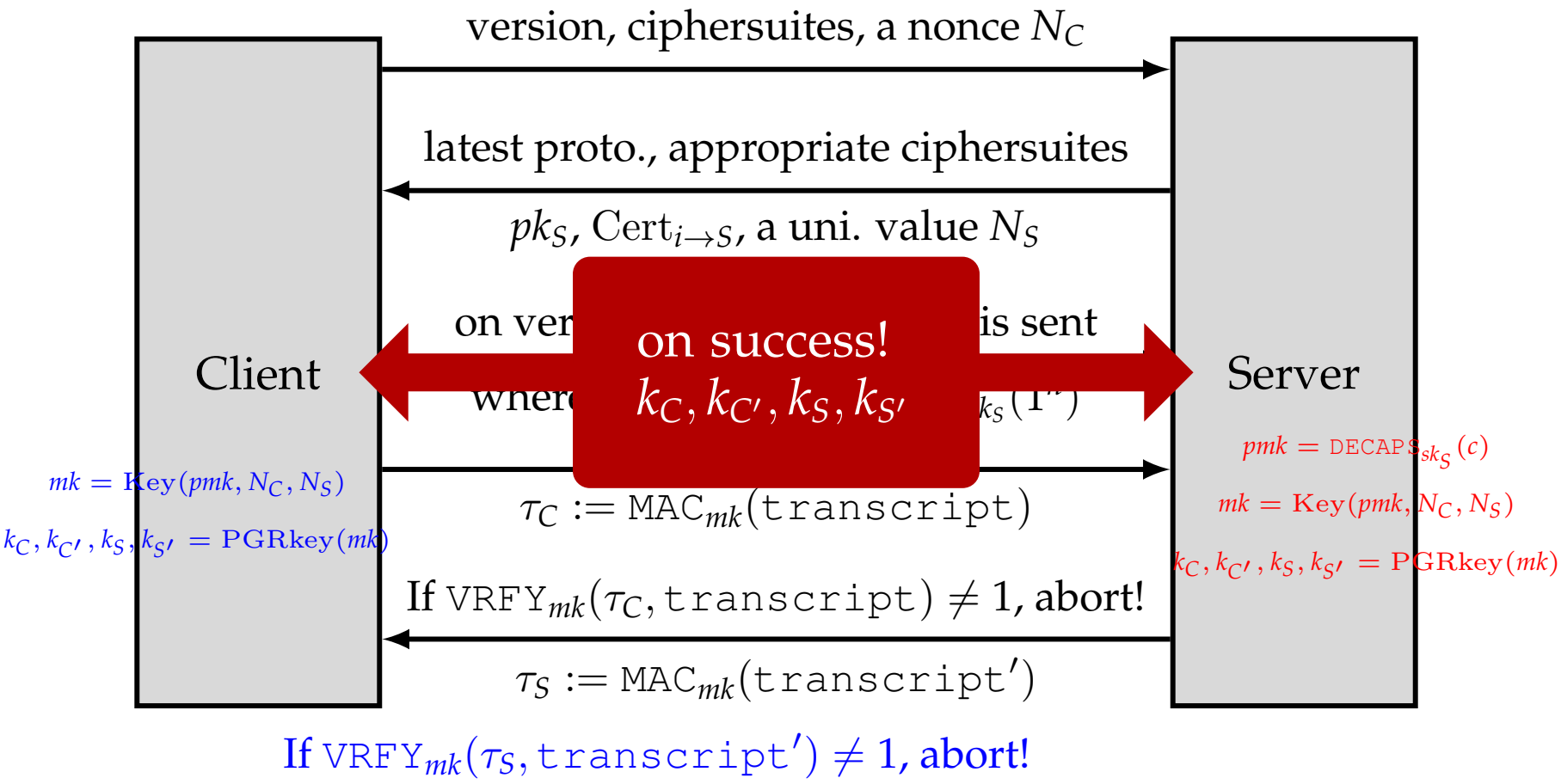


Handshake Protocol



If $\mathtt{VRFY}_{mk}(\tau_S, \mathtt{transcript}') \neq 1$, abort!

Handshake Protocol



Record-Layer Protocol

Once keys have been agreed upon by Client C and Server S, the parties use those keys to encrypt and authenticate all their subsequent communication.

- C uses k_C (resp., $k_{C'}$) to encrypt (resp., authenticate) all messages it sends to S.
- S uses k_S (resp., $k_{S'}$) to encrypt (resp., authenticate) all messages it sends to C.

Record-Layer Protocol

Once keys have been agreed upon by Client C and Server S, the parties use those keys to encrypt and authenticate all their subsequent communication.

- C uses k_C (resp., $k_{C'}$) to encrypt (resp., authenticate) all messages it sends to S.
- S uses k_S (resp., $k_{S'}$) to encrypt (resp., authenticate) all messages it sends to C.

Sequence numbers and directionality bits are used to prevent replay attacks, re-ordering and reflection attacks.

- Each party maintains two counters $\texttt{ctr}_{C,S}$ and $\texttt{ctr}_{S,C}$ keeping track of the number of messages sent from C to S and S to C) res. during the session.
- They also agree on a directionality bit $b_{C,S}$ and set $b_{S,C}$ to be its complement.