CTng: Secure Certificate and Revocation Transparency

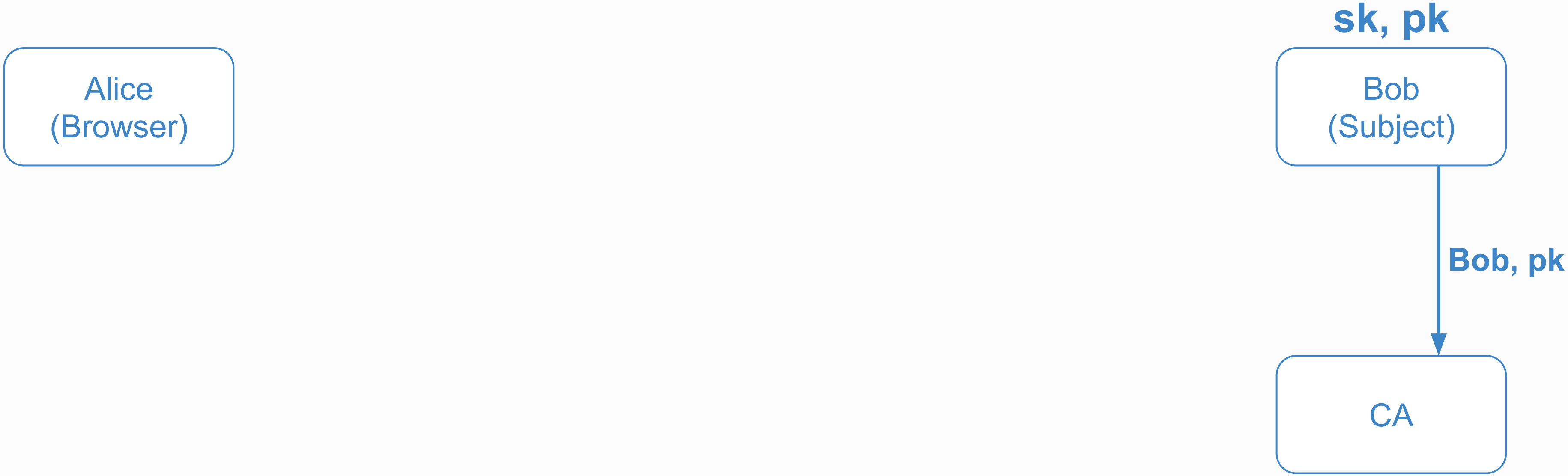
Jie Kong, Damon James, Hemi Leibowitz, Ewa Syta, Amir Herzberg

NDSS 2026

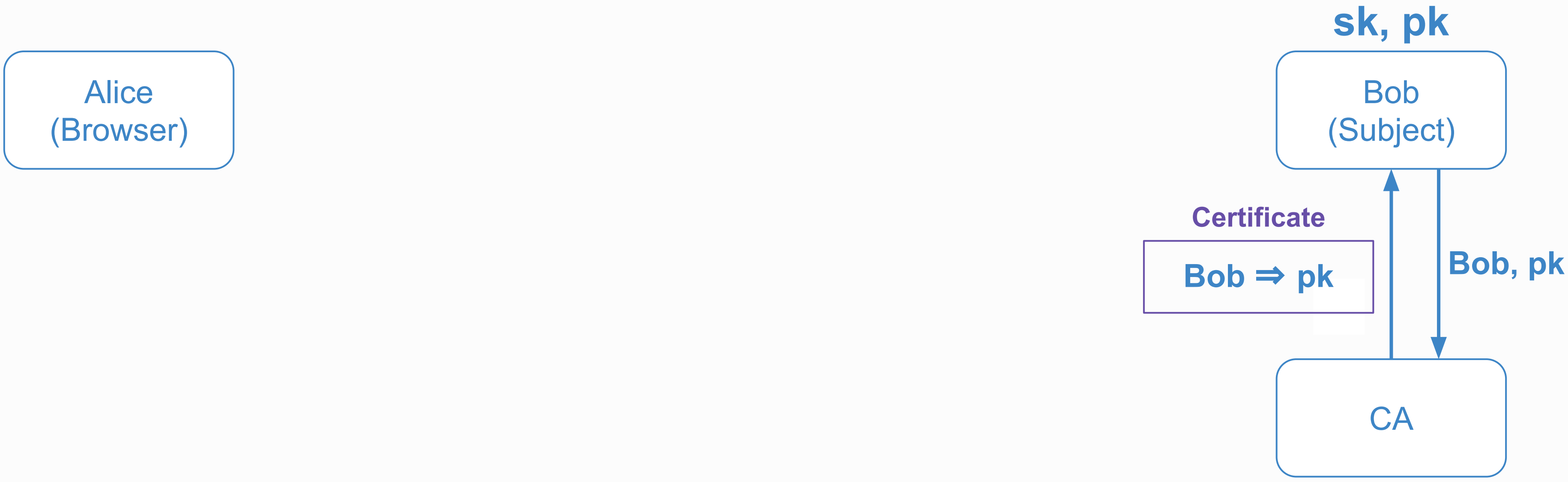
Agenda

- Challenges in securing the current Web-PKI
  - Brief overview of Web-PKI (X.509 + CT + Vendor-assisted revocation)
  - Revocation is broken
  - Efficiency, security and privacy issues regarding Certificate Transparency (CT)
- CTng
  - Efficient and secure transparency and revocation
  - Protects relying parties’ privacy

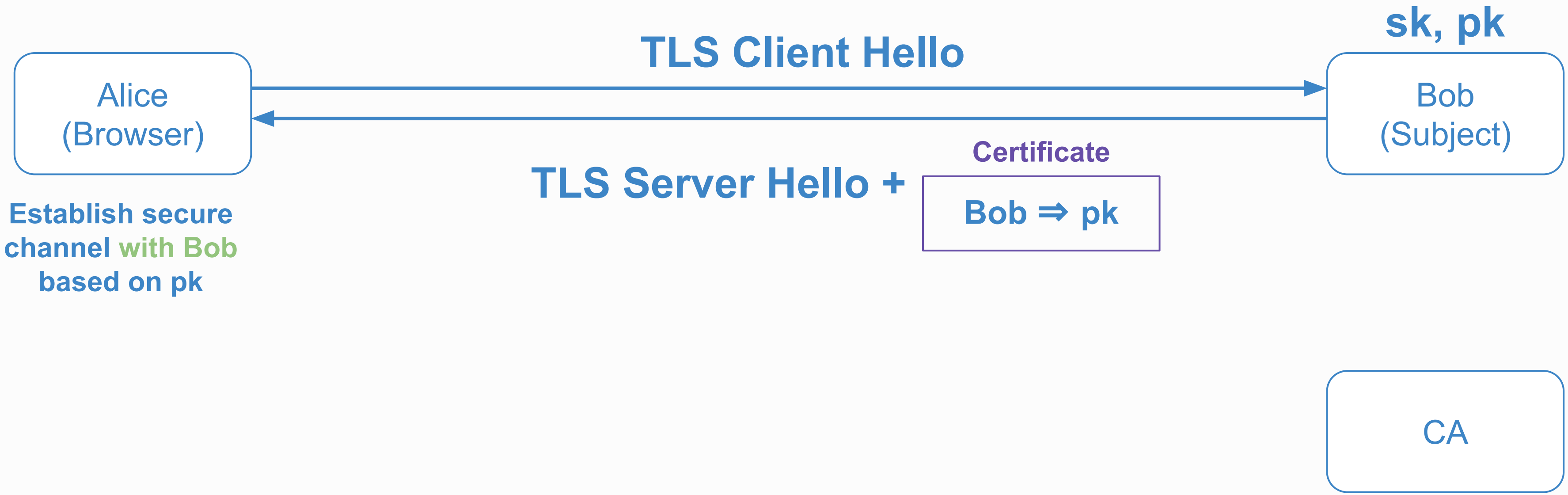
Web-PKI (X.509 + CT + Vendor-assisted revocation)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



Alice (Browser)

TLS Client Hello

sk, pk

Bob (Subject)

TLS Server Hello + Certificate

Bob ⇒ pk

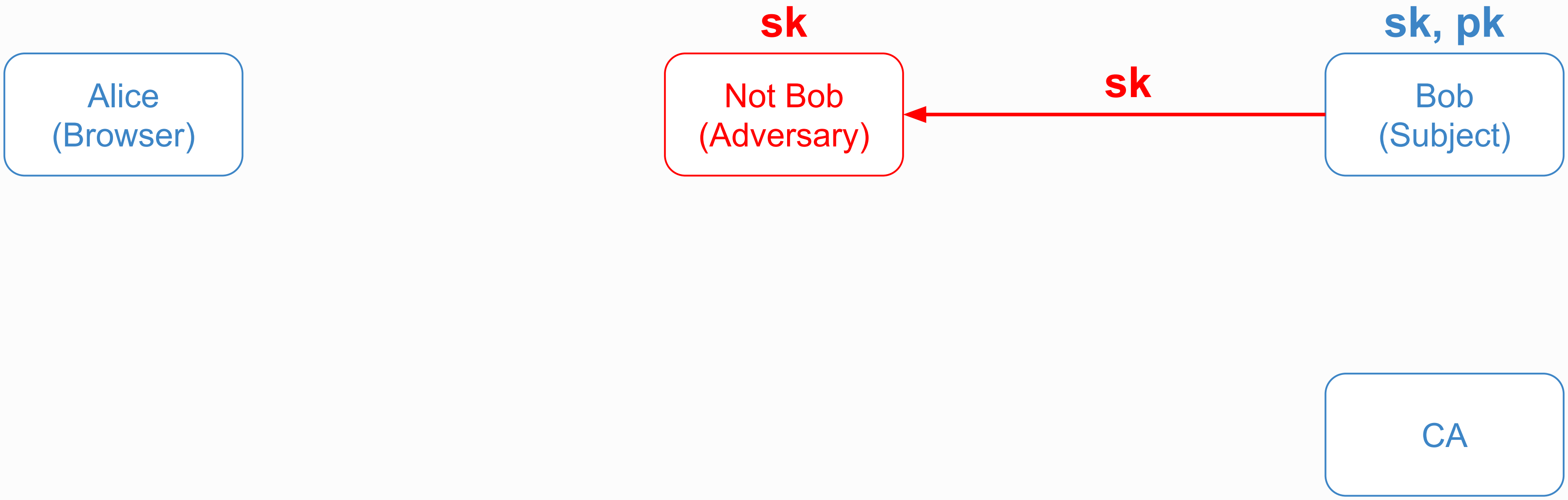
Establish secure channel with Bob based on pk

CA

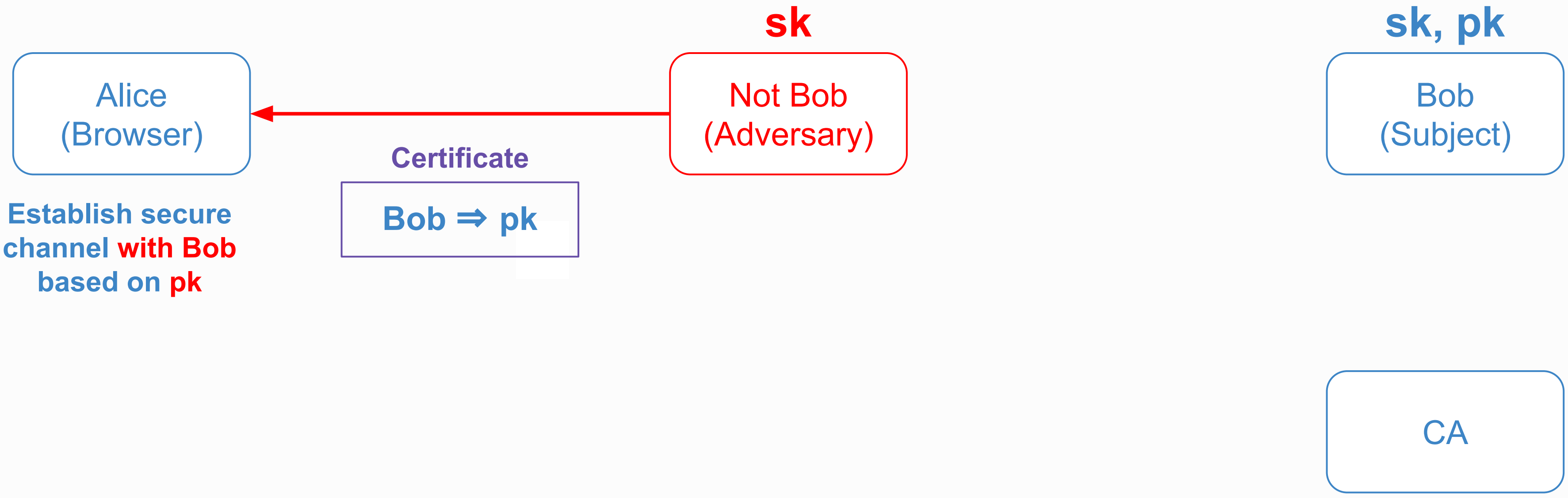
Revocation Challenges

sk, pk
Alice
(Browser)
Bob
(Subject)
CA

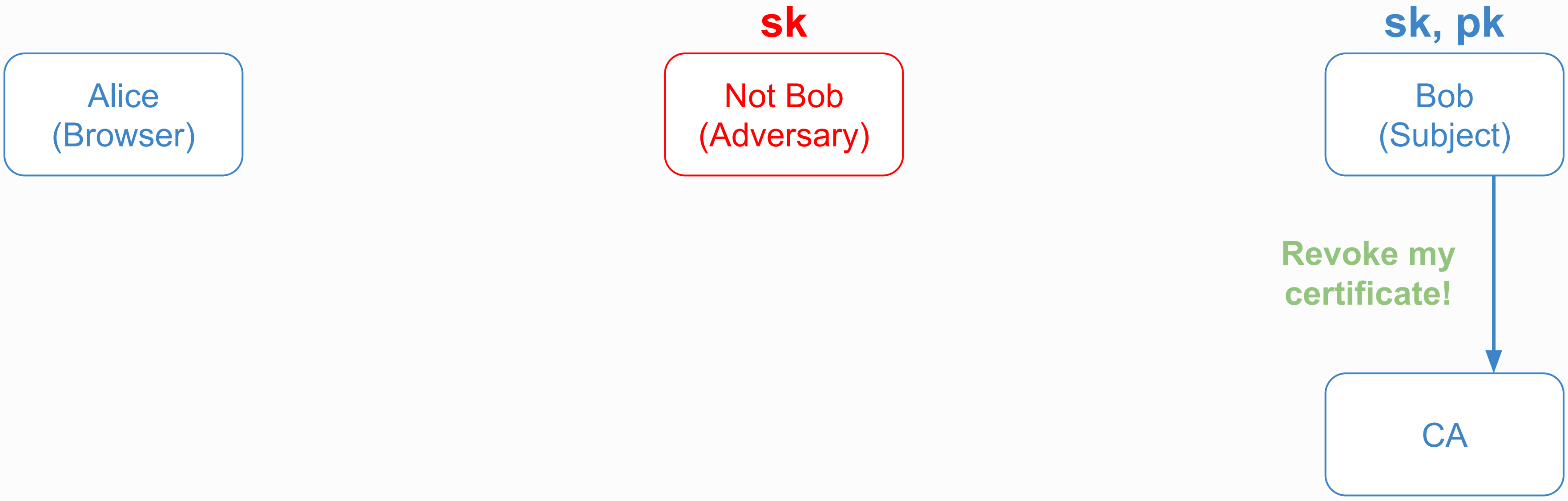
Revocation Challenges



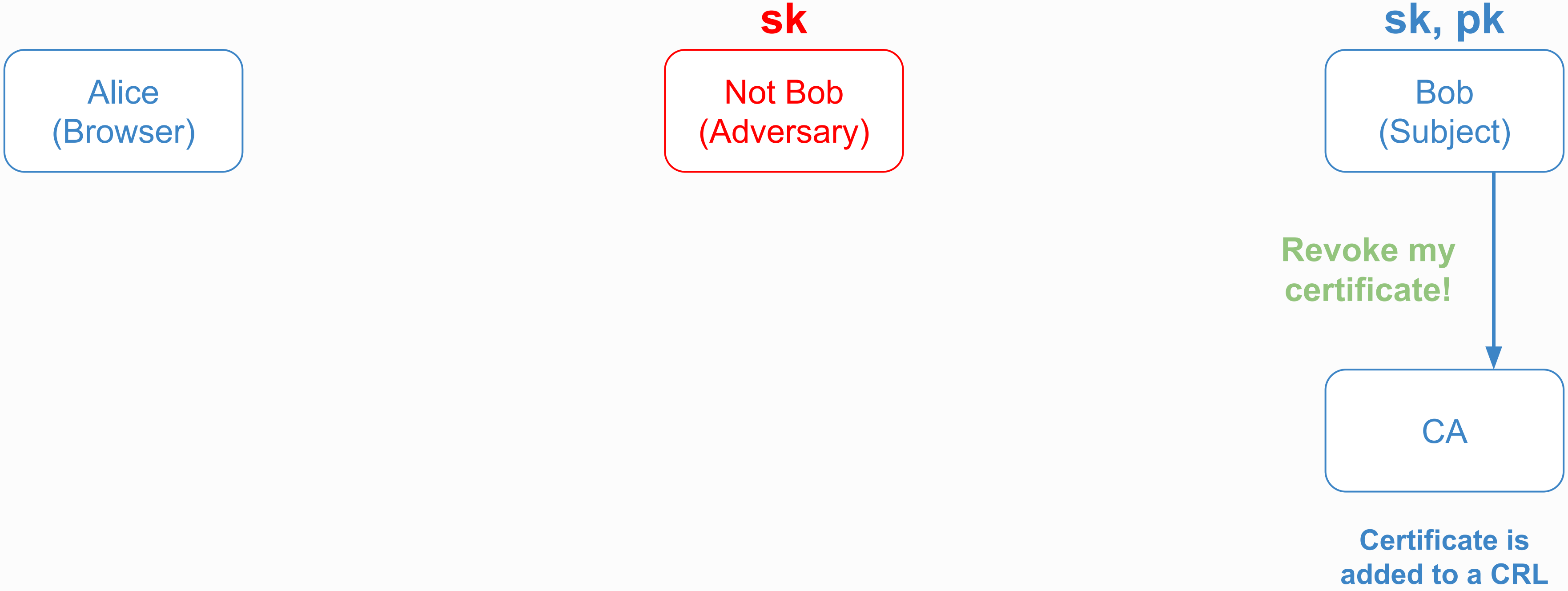
Revocation Challenges



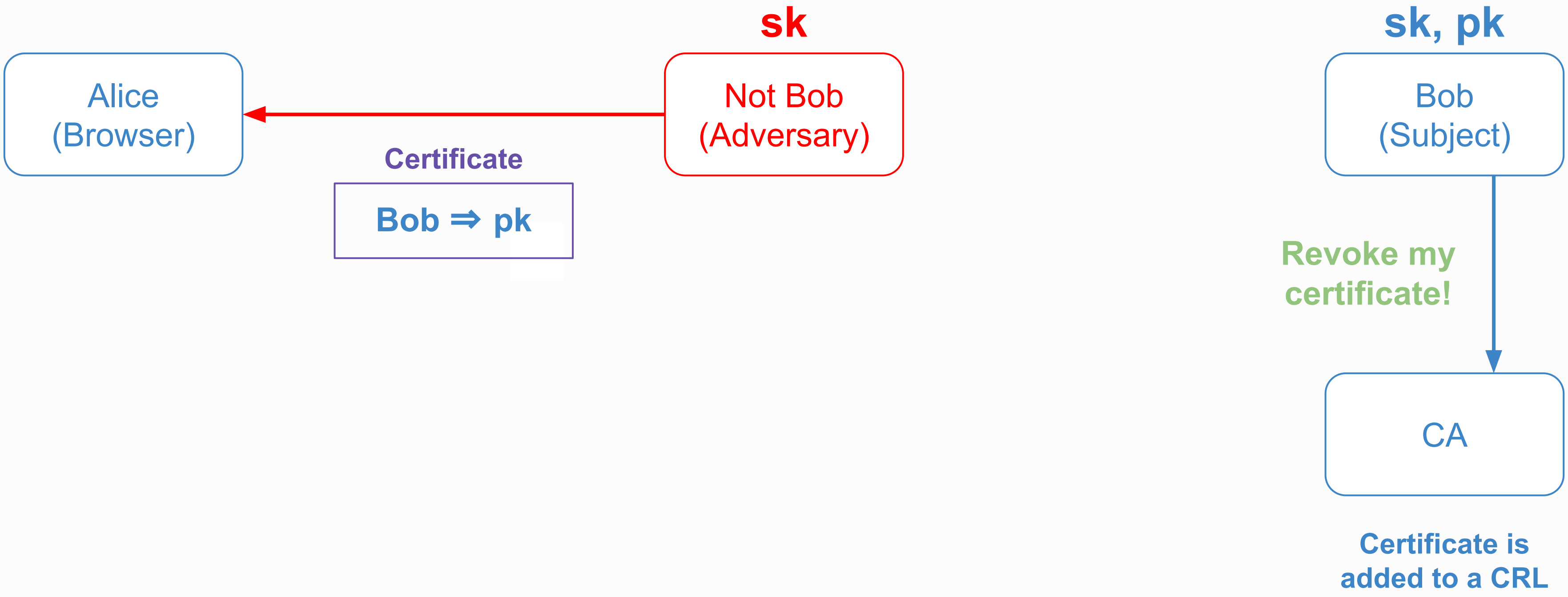
Revocation Challenges



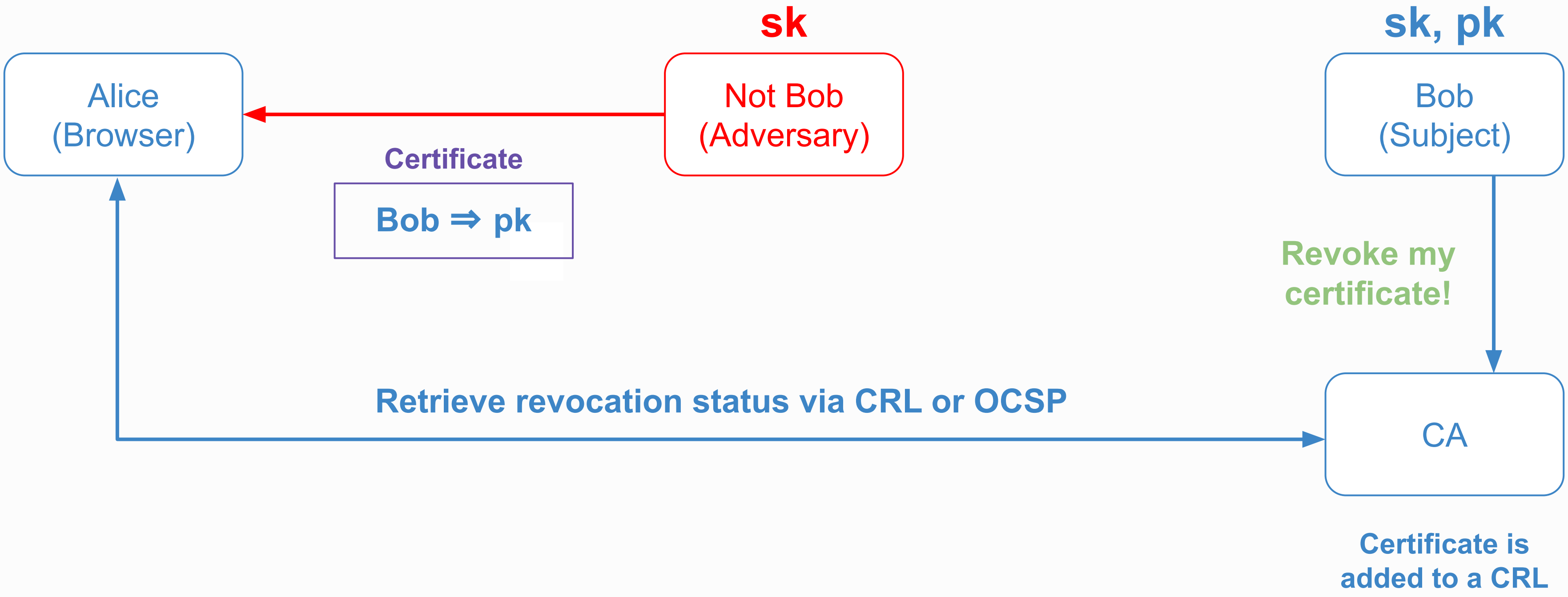
Revocation Challenges



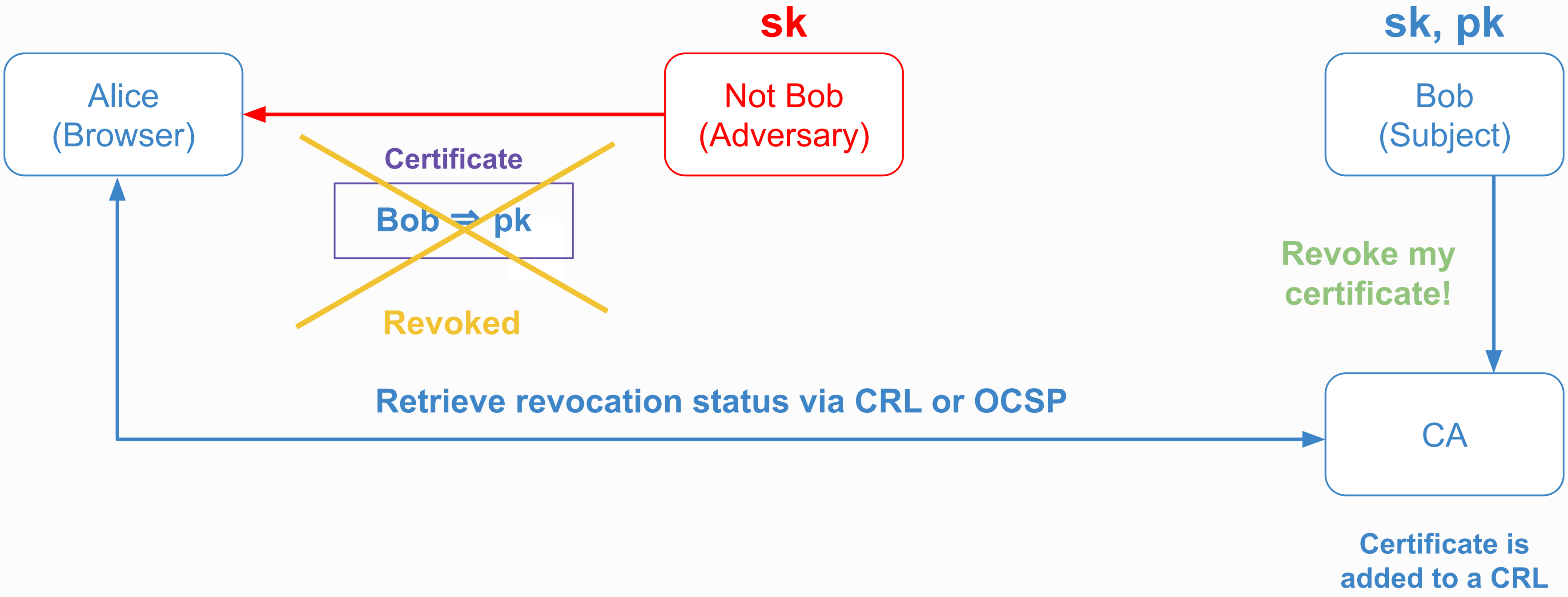
Revocation Challenges



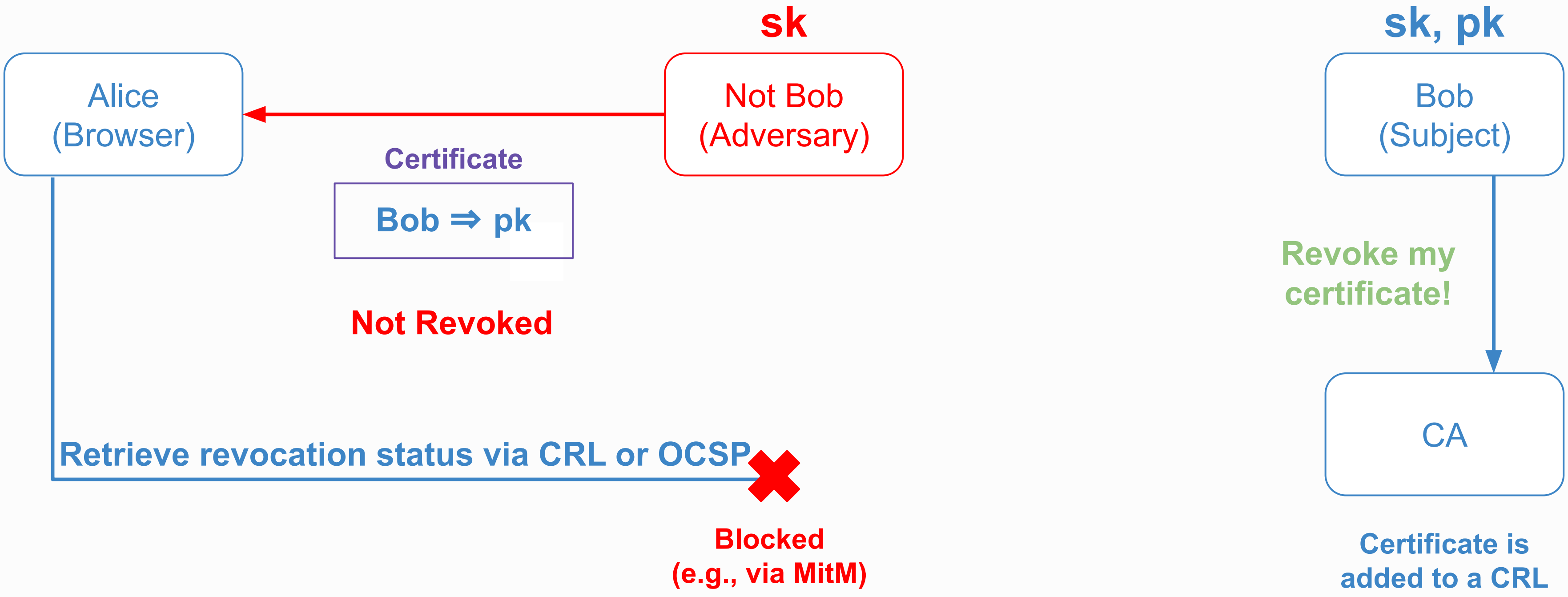
Revocation Challenges



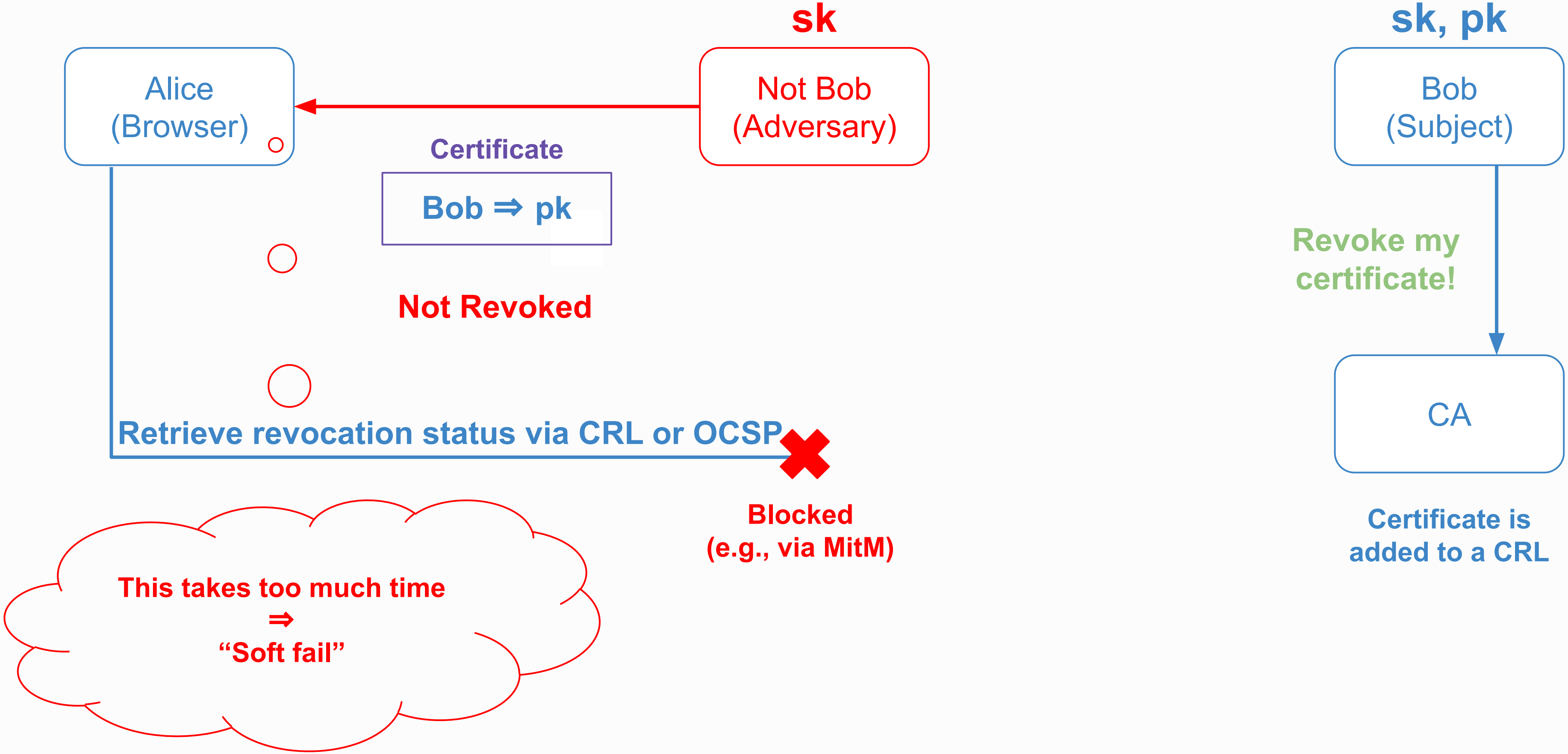
Revocation Challenges



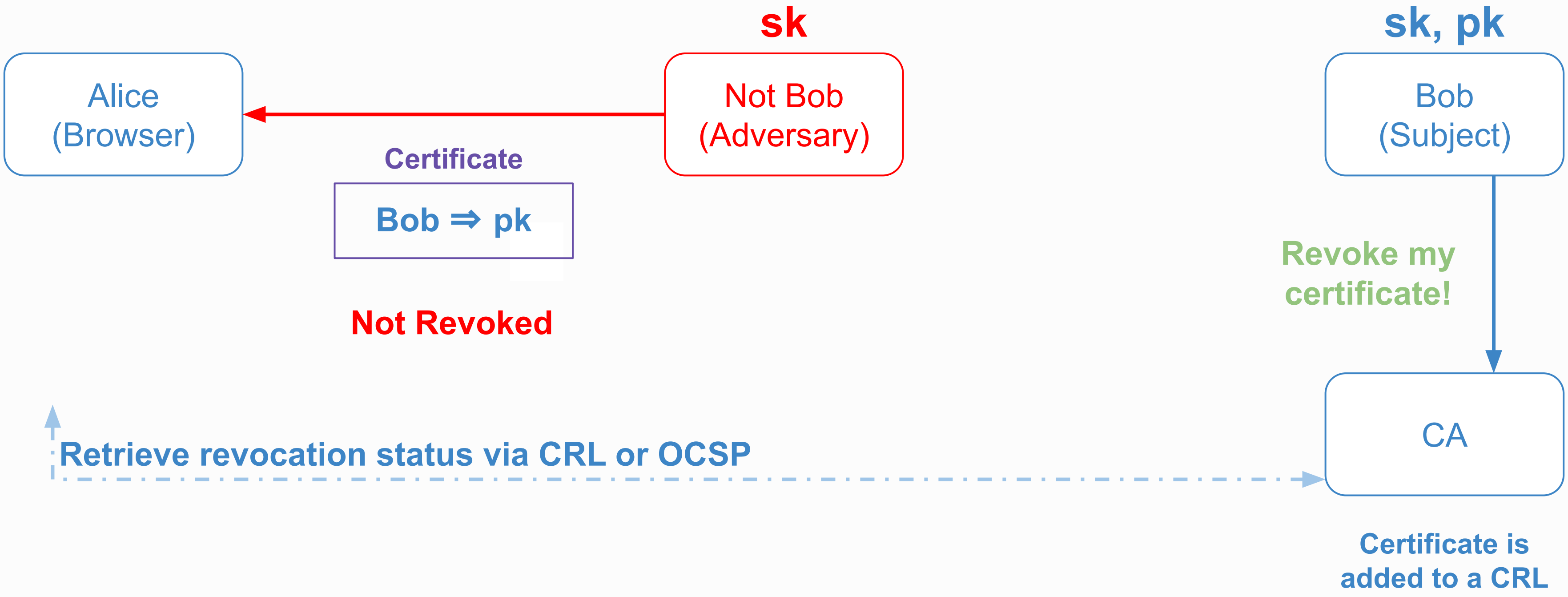
Revocation Challenges (Soft fail)



Revocation Challenges (Soft fail)



Revocation Challenges (Soft fail)



sk

sk, pk

Alice
(Browser)

Not Bob
(Adversary)

Bob
(Subject)

Certificate

Bob ⇒ pk

Not Revoked

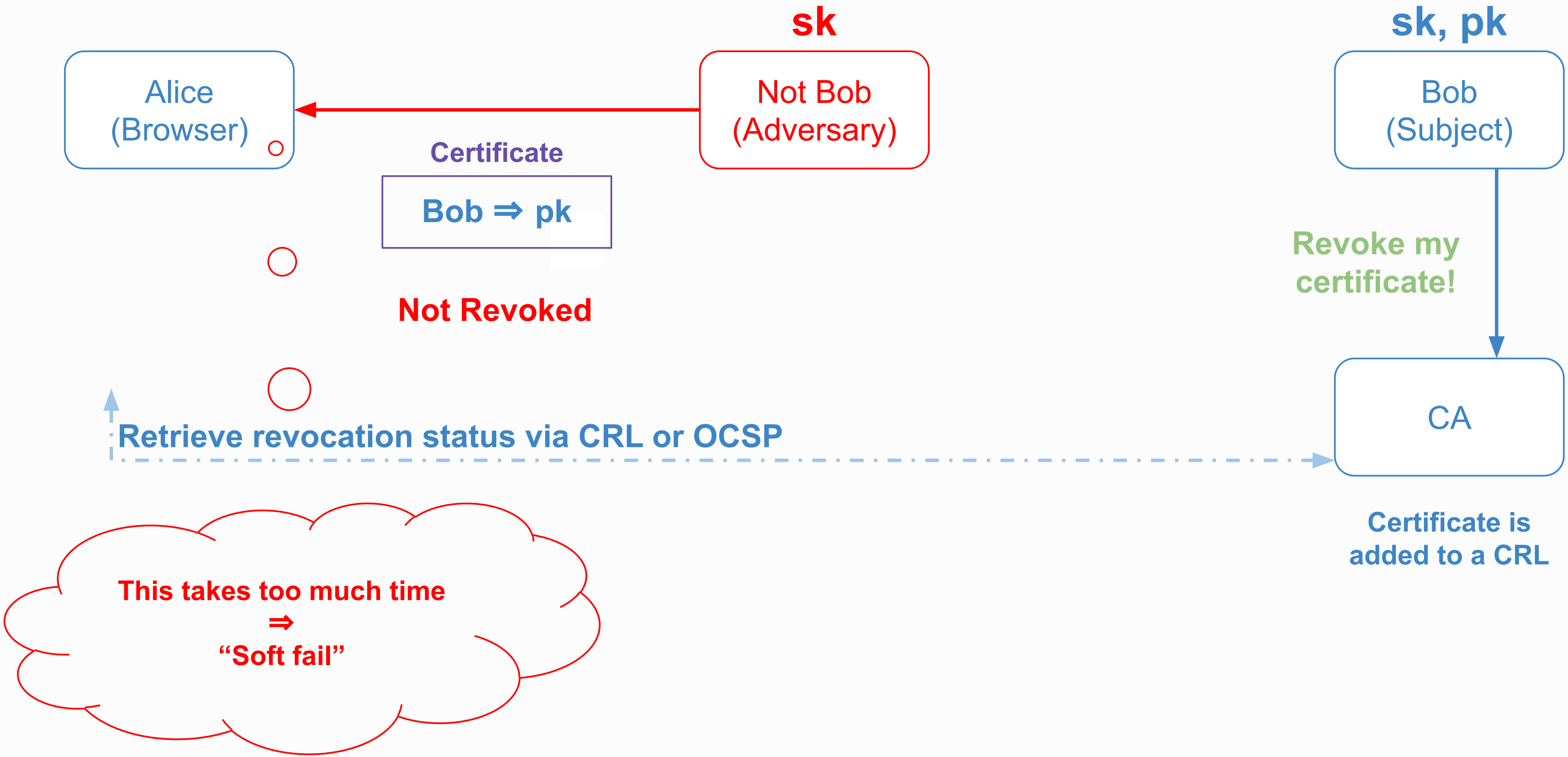
Revoke my certificate!

CA

Retrieve revocation status via CRL or OCSP

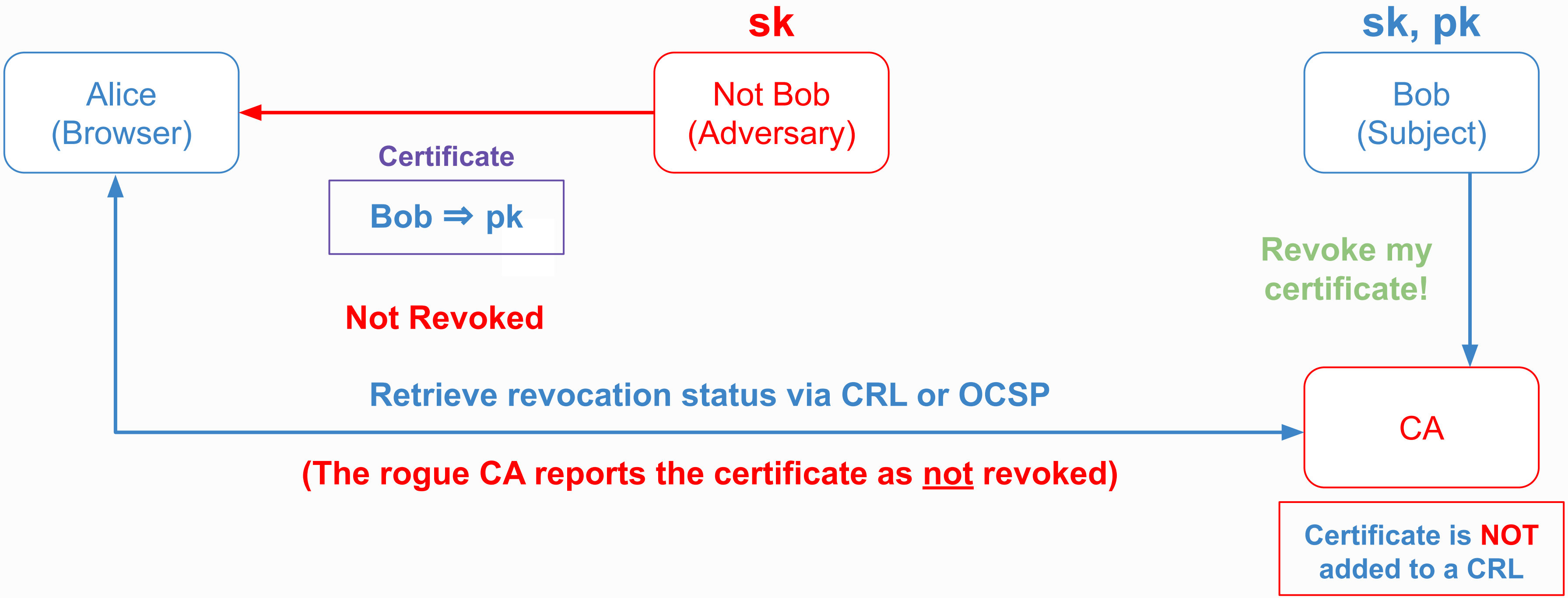
Certificate is added to a CRL

Revocation Challenges (Soft fail)



This takes too much time
⇒
“Soft fail”

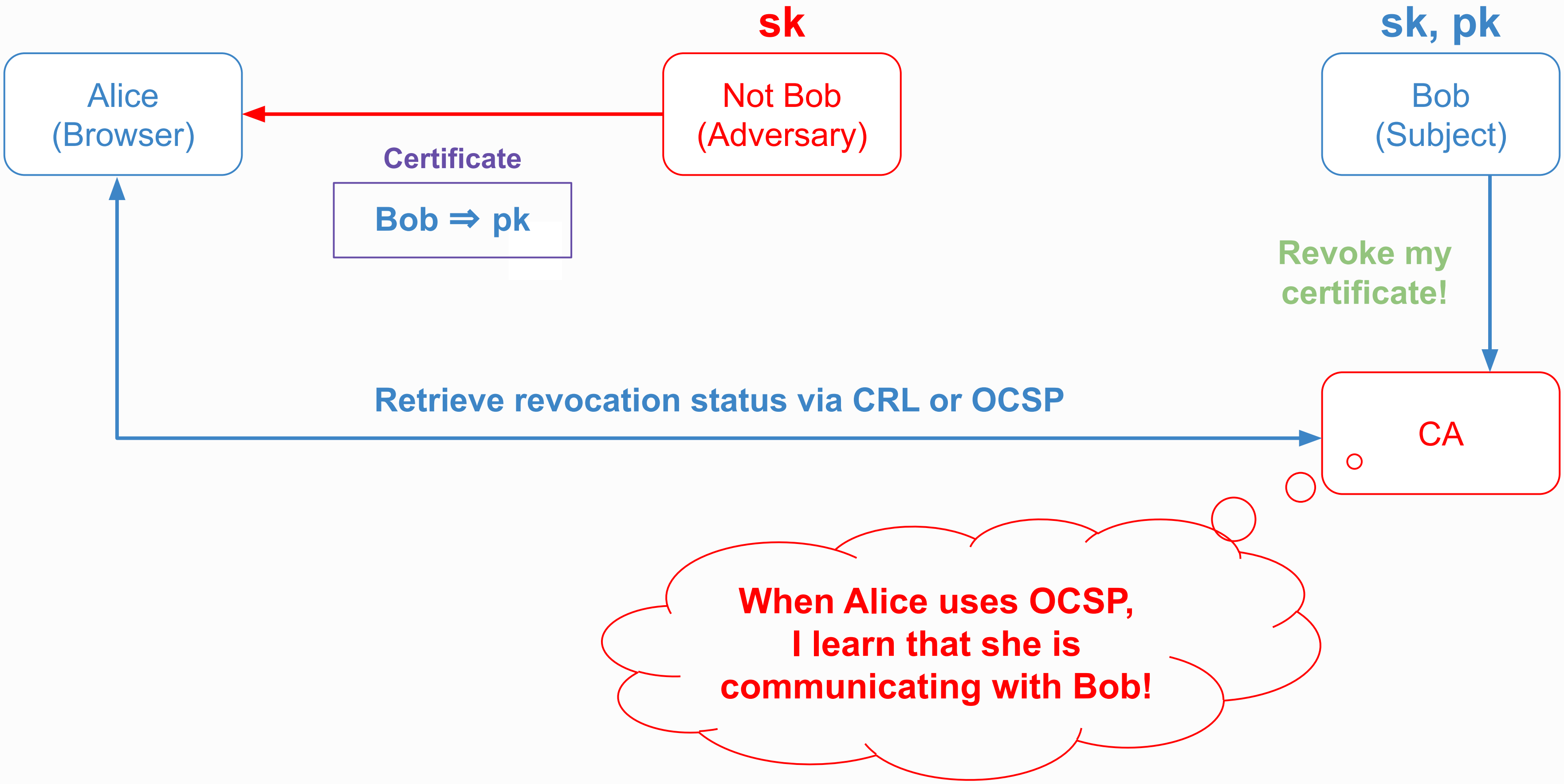
Revocation Challenges (Rogue CA)



(The rogue CA reports the certificate as not revoked)

Certificate is NOT added to a CRL

Revocation Challenges (Snoopy CA compromises privacy)



sk

sk, pk

Alice (Browser)

Not Bob (Adversary)

Bob (Subject)

Certificate

Bob ⇒ pk

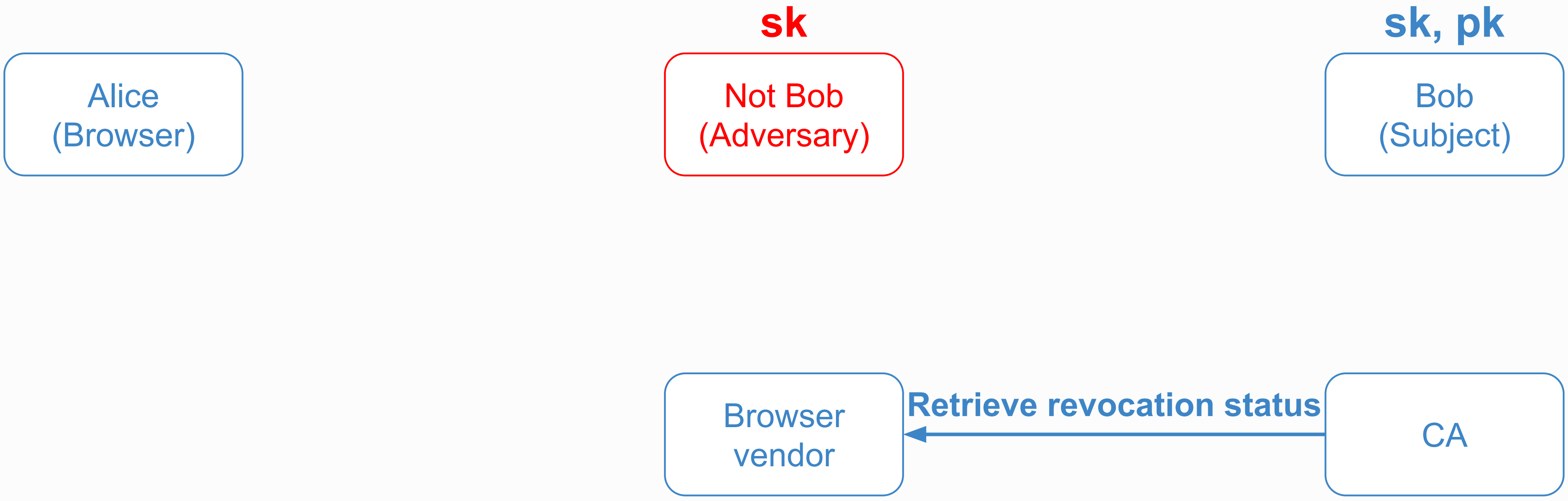
Revoke my certificate!

Retrieve revocation status via CRL or OCSP

CA

When Alice uses OCSP, I learn that she is communicating with Bob!

Web-PKI (X.509 + CT + Vendor-assisted revocation)



sk

sk, pk

Alice (Browser)

Not Bob (Adversary)

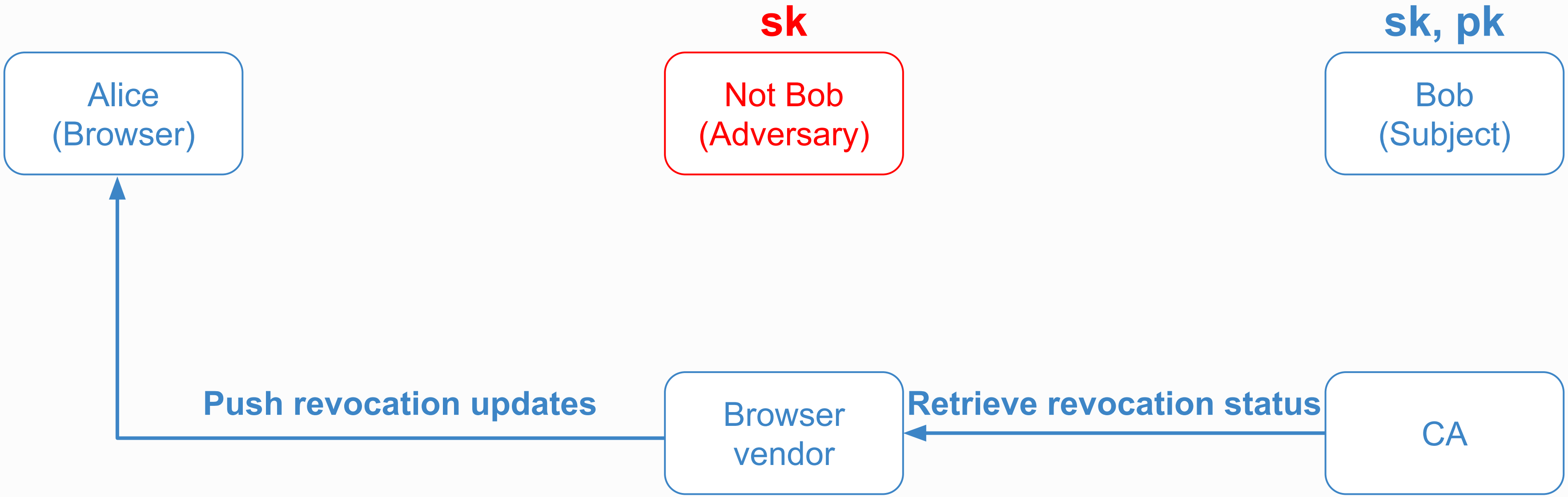
Bob (Subject)

Browser vendor

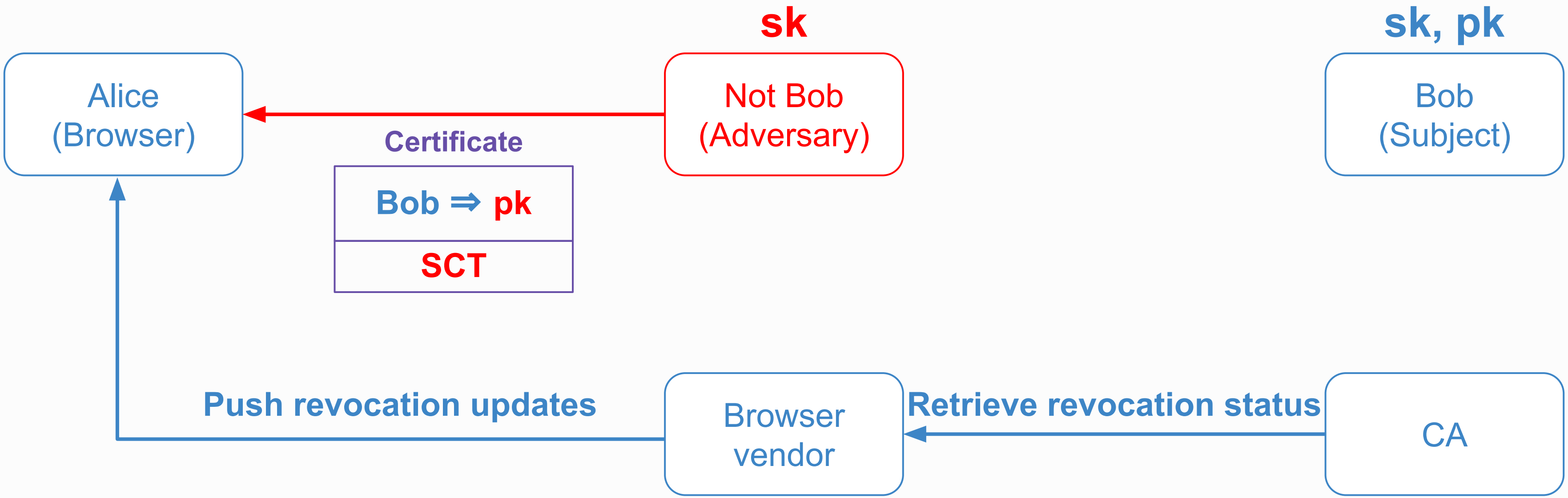
Retrieve revocation status

CA

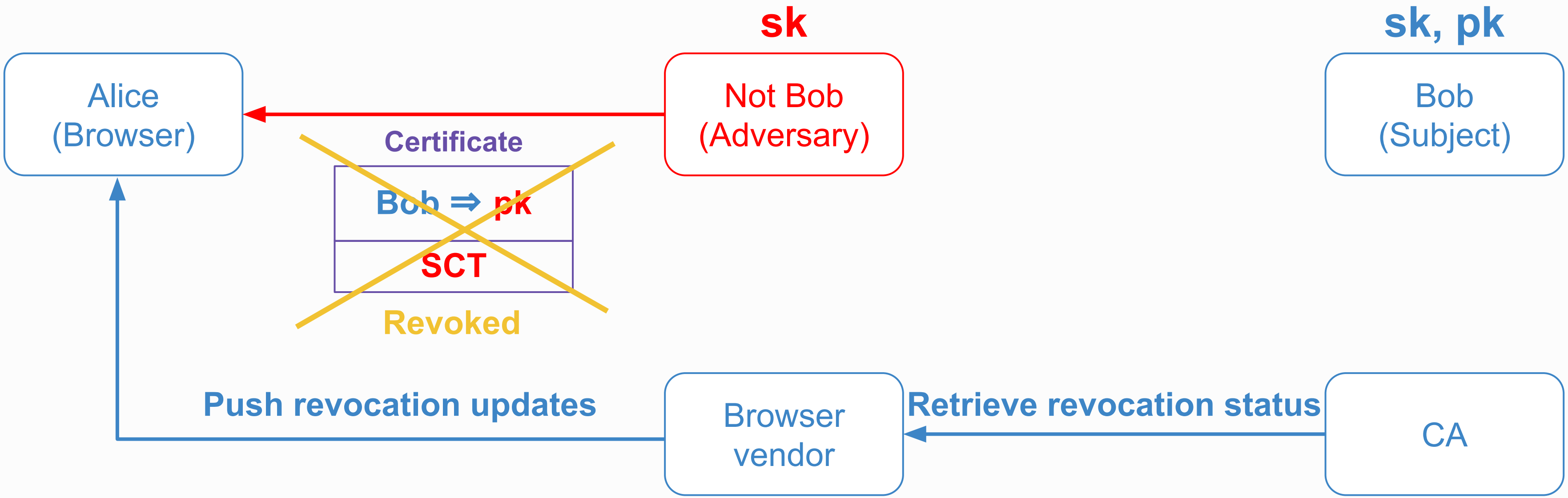
Web-PKI (X.509 + CT + Vendor-assisted revocation)



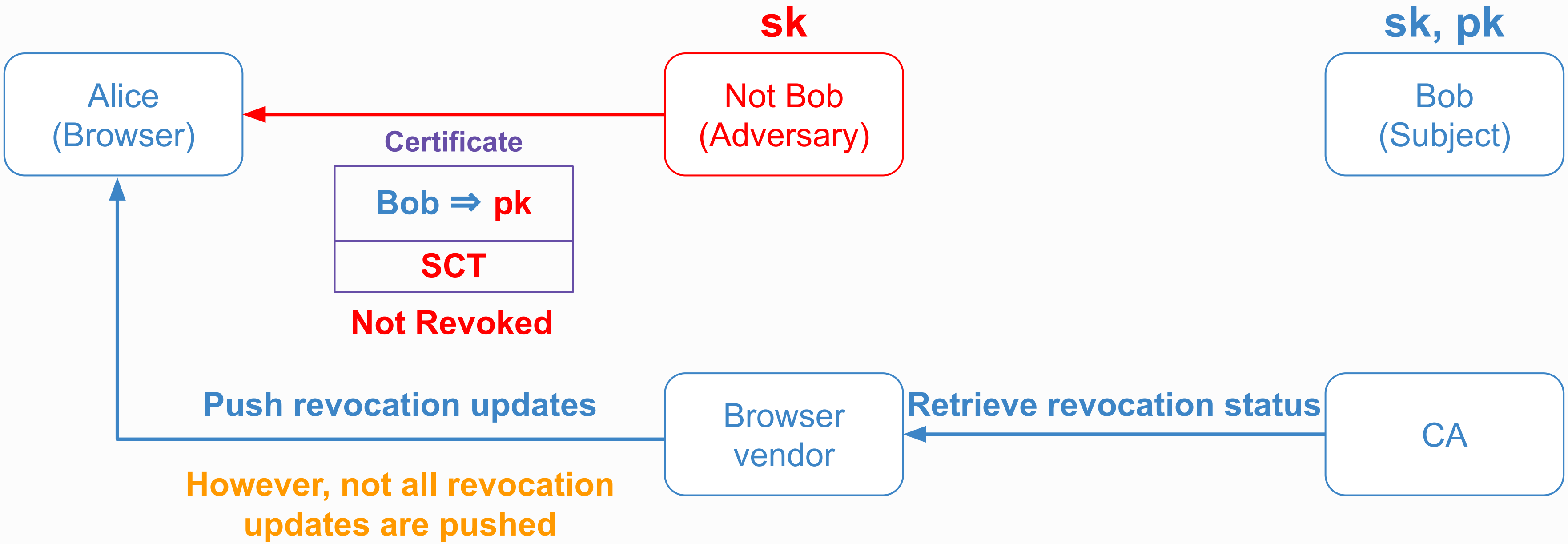
Web-PKI (X.509 + CT + Vendor-assisted revocation)



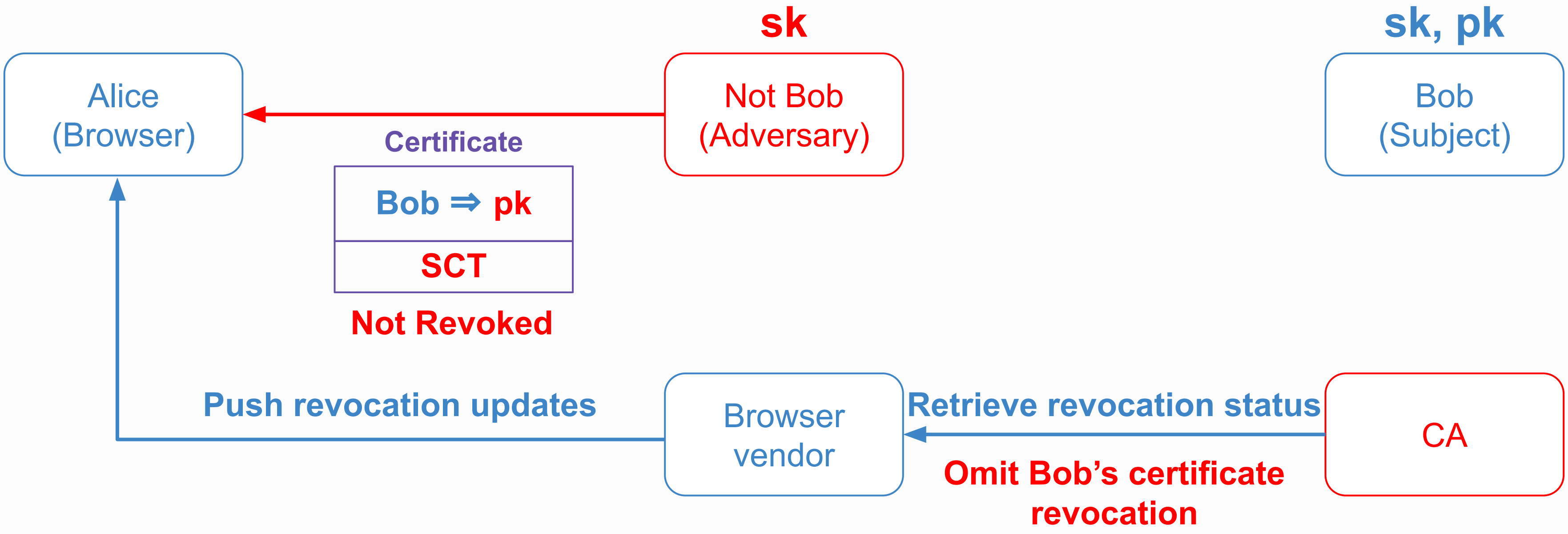
Web-PKI (X.509 + CT + Vendor-assisted revocation)



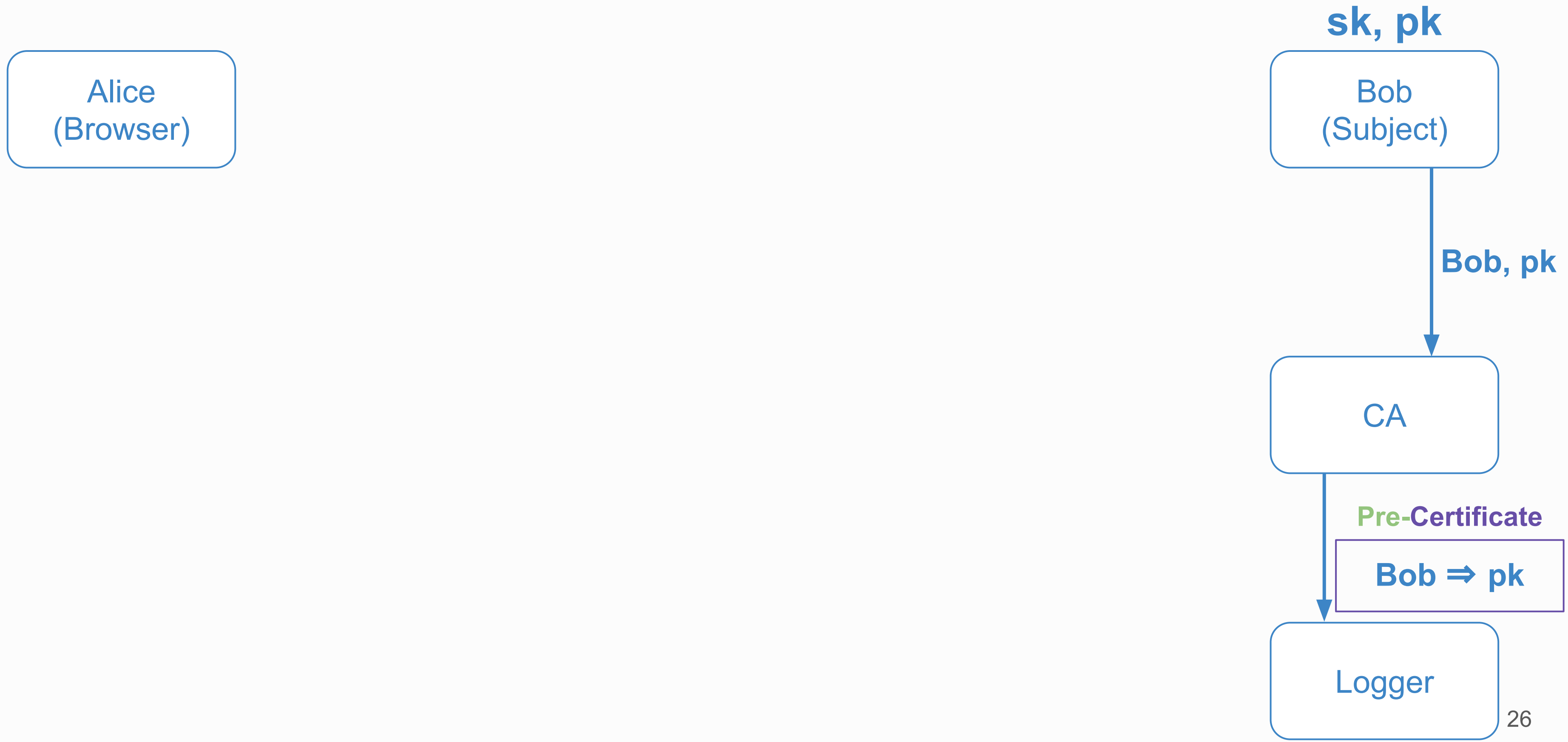
Revocation Challenges (Selective updates)



Revocation Challenges (Rogue CA)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



Alice (Browser)

sk, pk

Bob (Subject)

Bob, pk

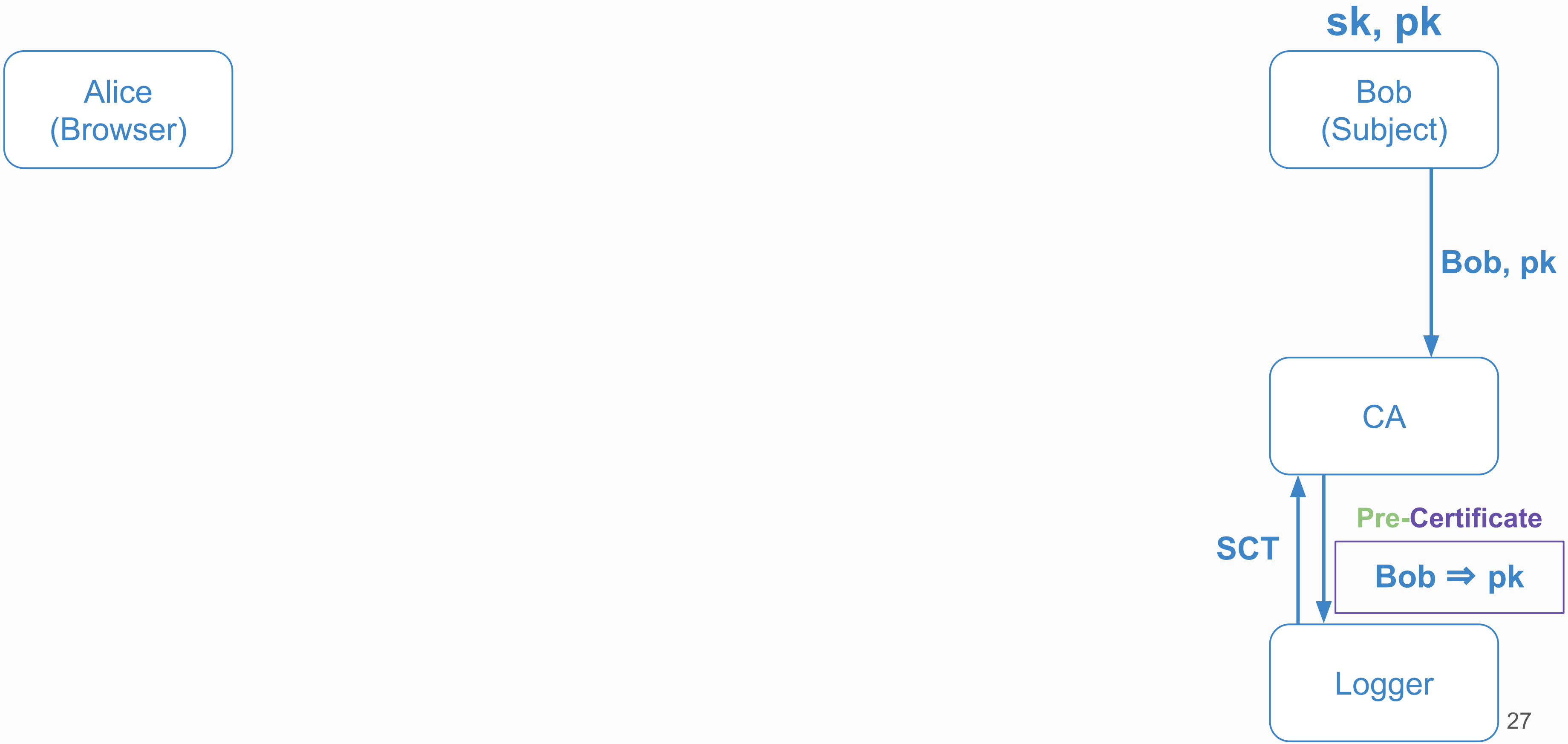
CA

Pre-Certificate

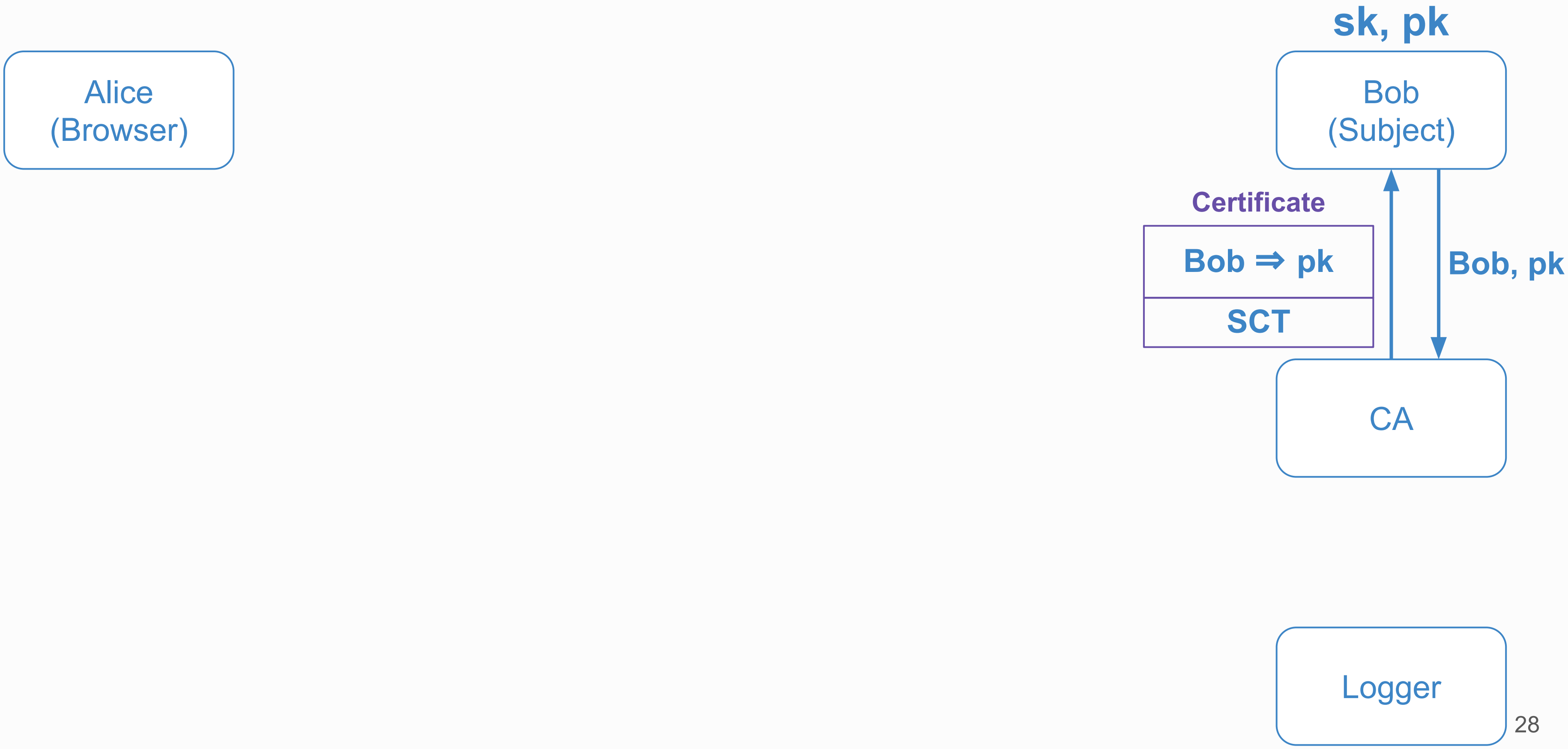
Bob ⇒ pk

Logger

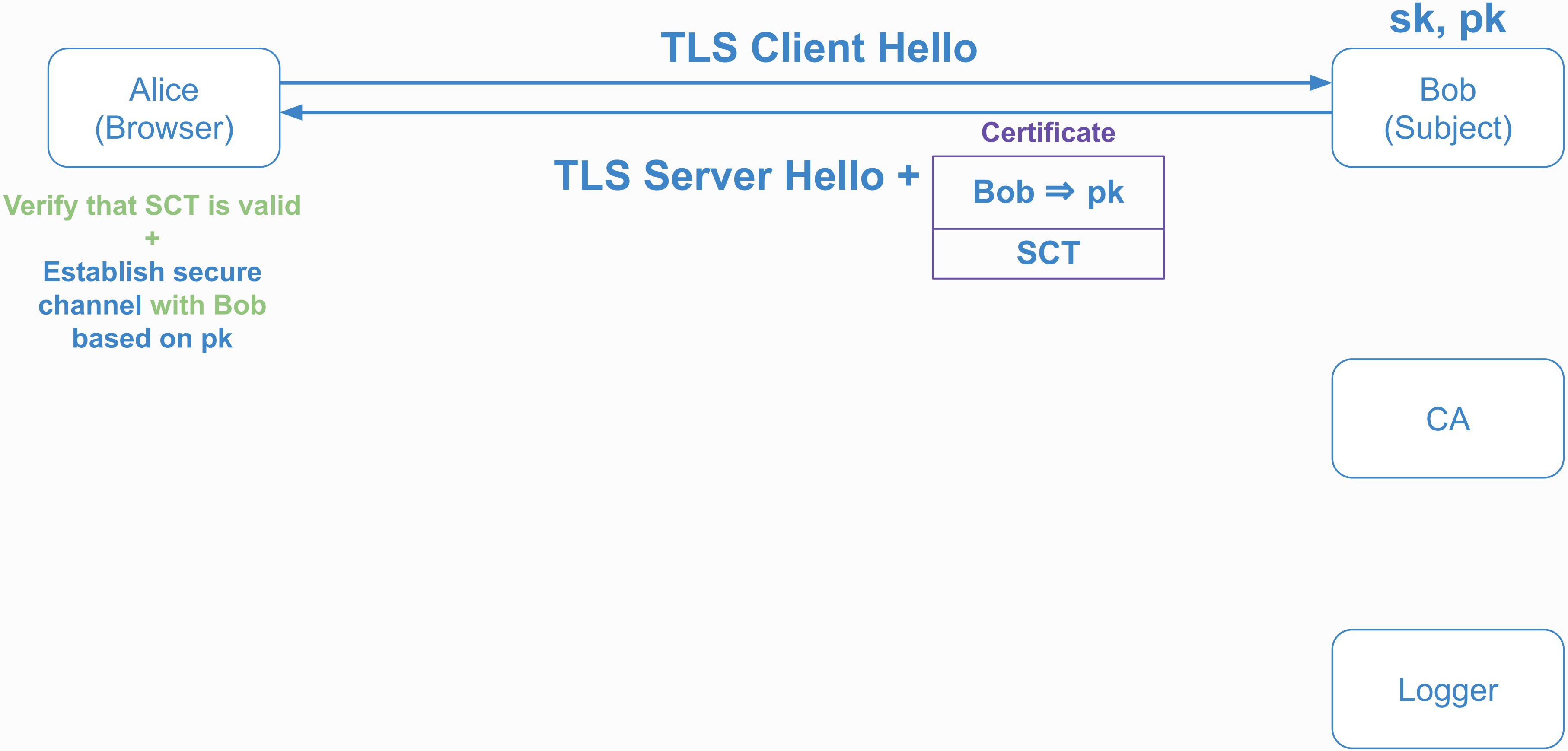
Web-PKI (X.509 + CT + Vendor-assisted revocation)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



sk, pk

TLS Client Hello

Alice
(Browser)

Bob
(Subject)

TLS Server Hello +

Certificate

Bob ⇒ pk

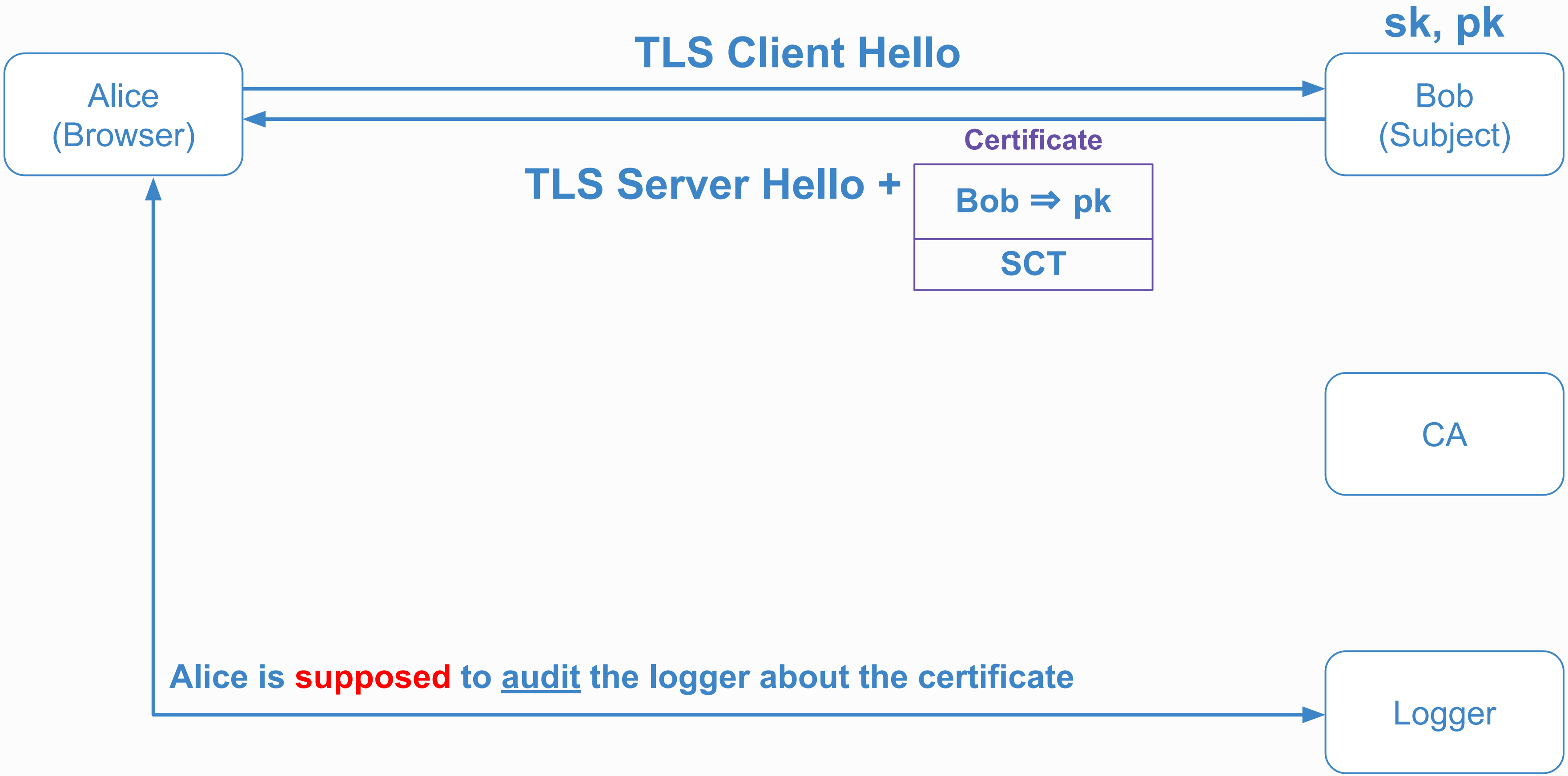
SCT

Verify that SCT is valid
+
Establish secure channel with Bob based on pk

CA

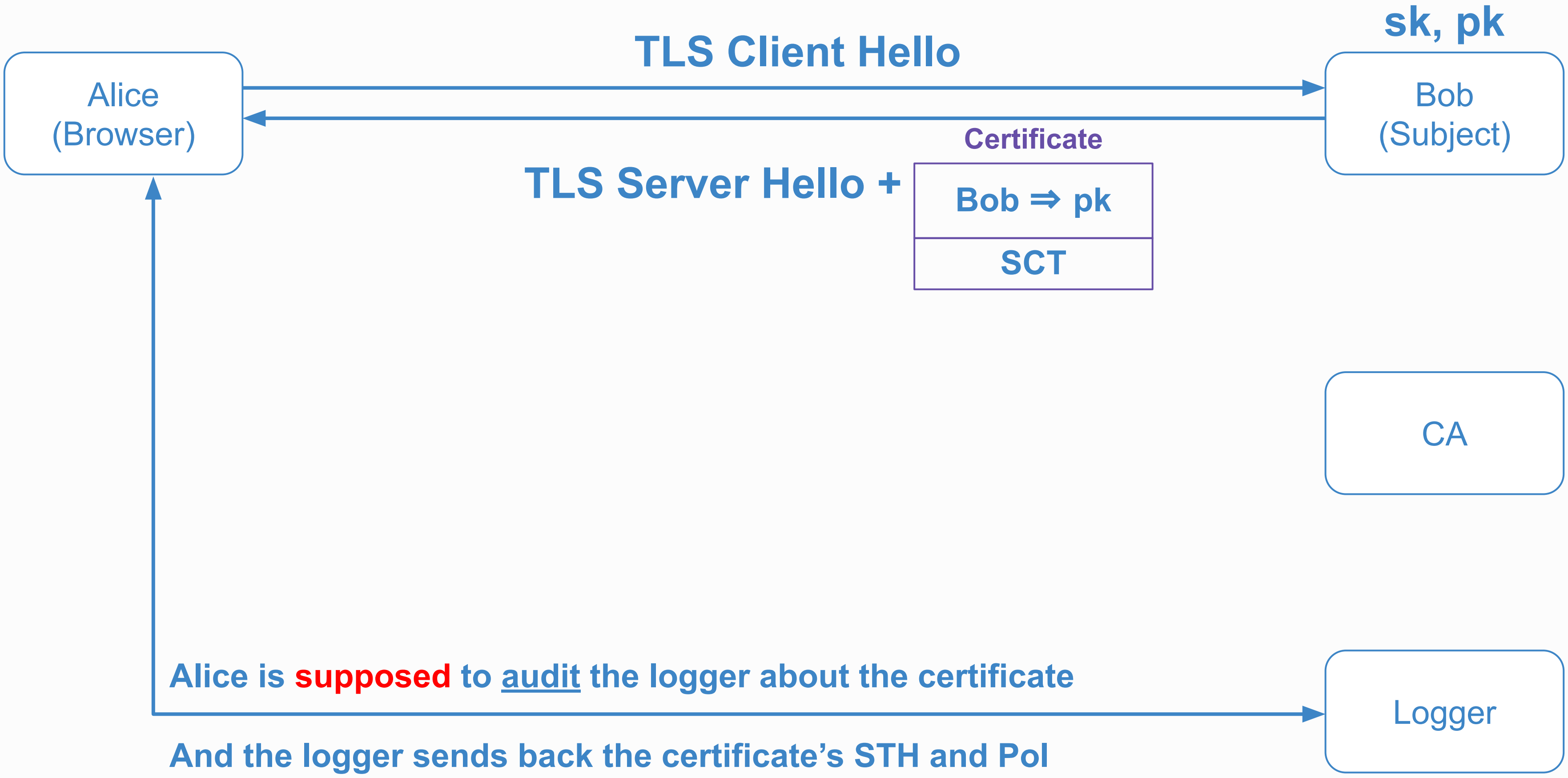
Logger

Web-PKI (X.509 + CT + Vendor-assisted revocation)



Alice is **supposed** to audit the logger about the certificate

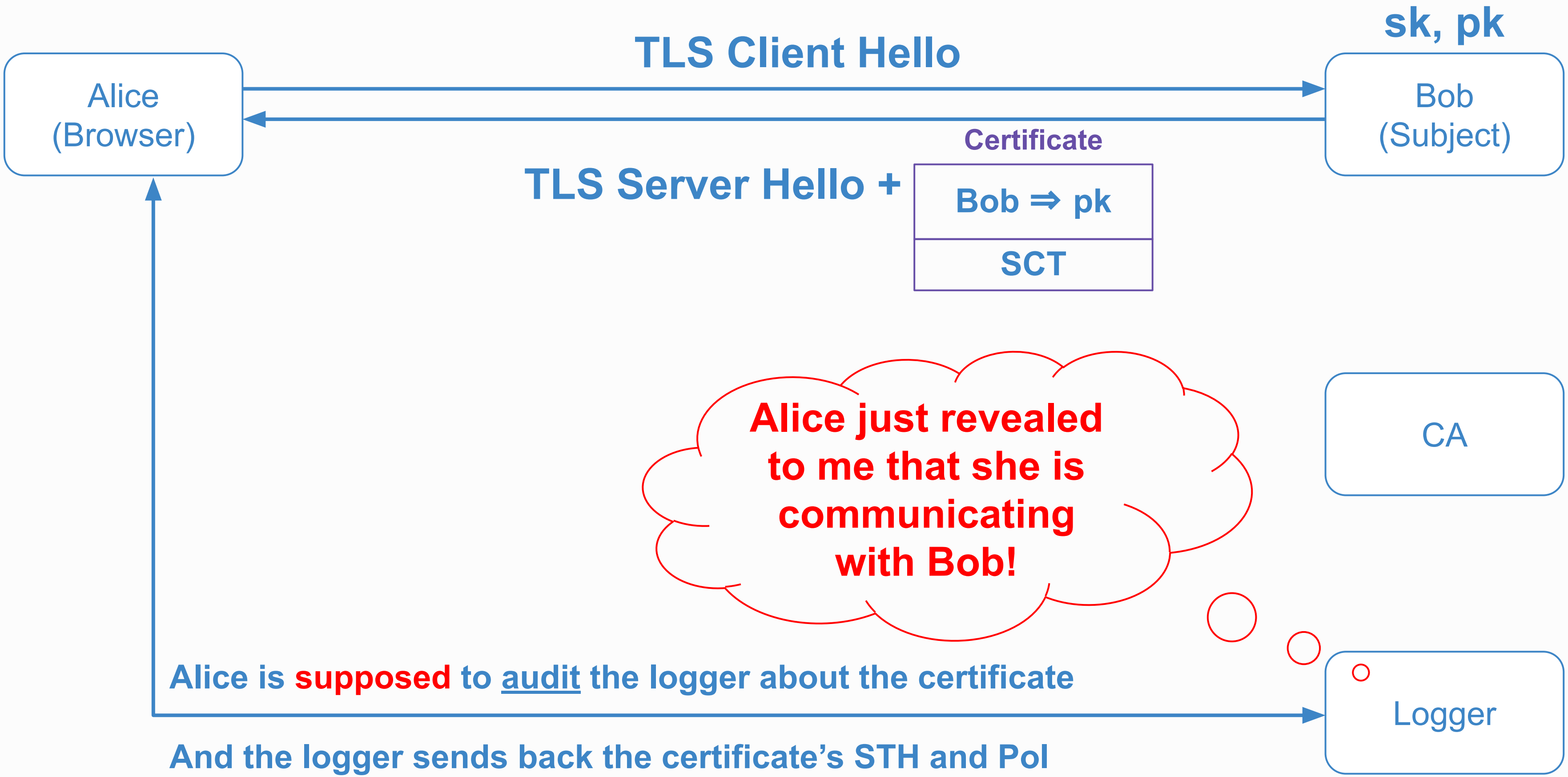
Web-PKI (X.509 + CT + Vendor-assisted revocation)



Alice is **supposed** to audit the logger about the certificate

And the logger sends back the certificate's STH and PoI

Web-PKI (X.509 + CT + Vendor-assisted revocation)



sk, pk

TLS Client Hello

Alice (Browser)

Bob (Subject)

TLS Server Hello +

Certificate

Bob ⇒ pk

SCT

Alice just revealed to me that she is communicating with Bob!

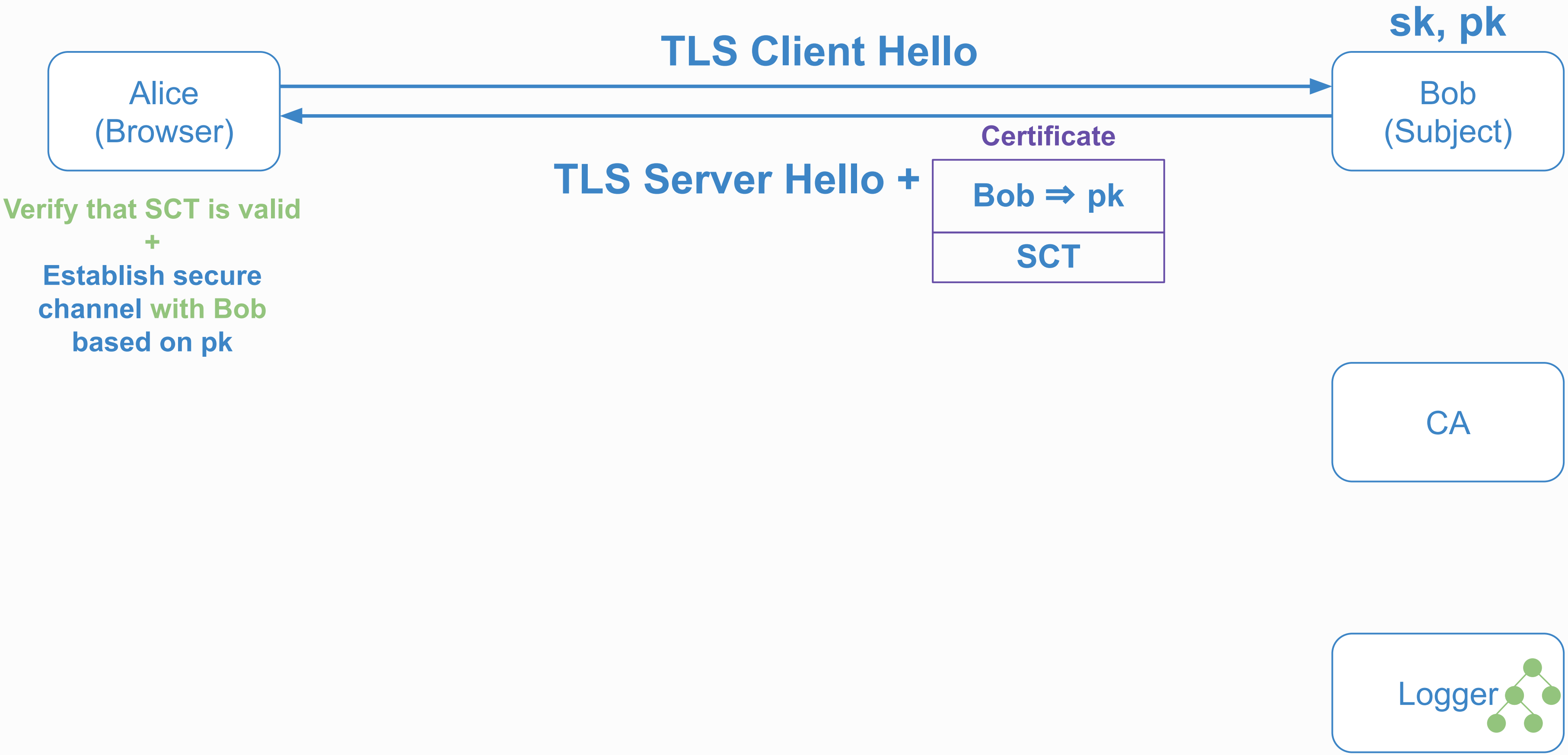
CA

Logger

Alice is supposed to audit the logger about the certificate

And the logger sends back the certificate’s STH and PoI

Web-PKI (X.509 + CT + Vendor-assisted revocation)



sk, pk

TLS Client Hello

Alice (Browser)

Bob (Subject)

TLS Server Hello +

Certificate

Bob ⇒ pk

SCT

Verify that SCT is valid

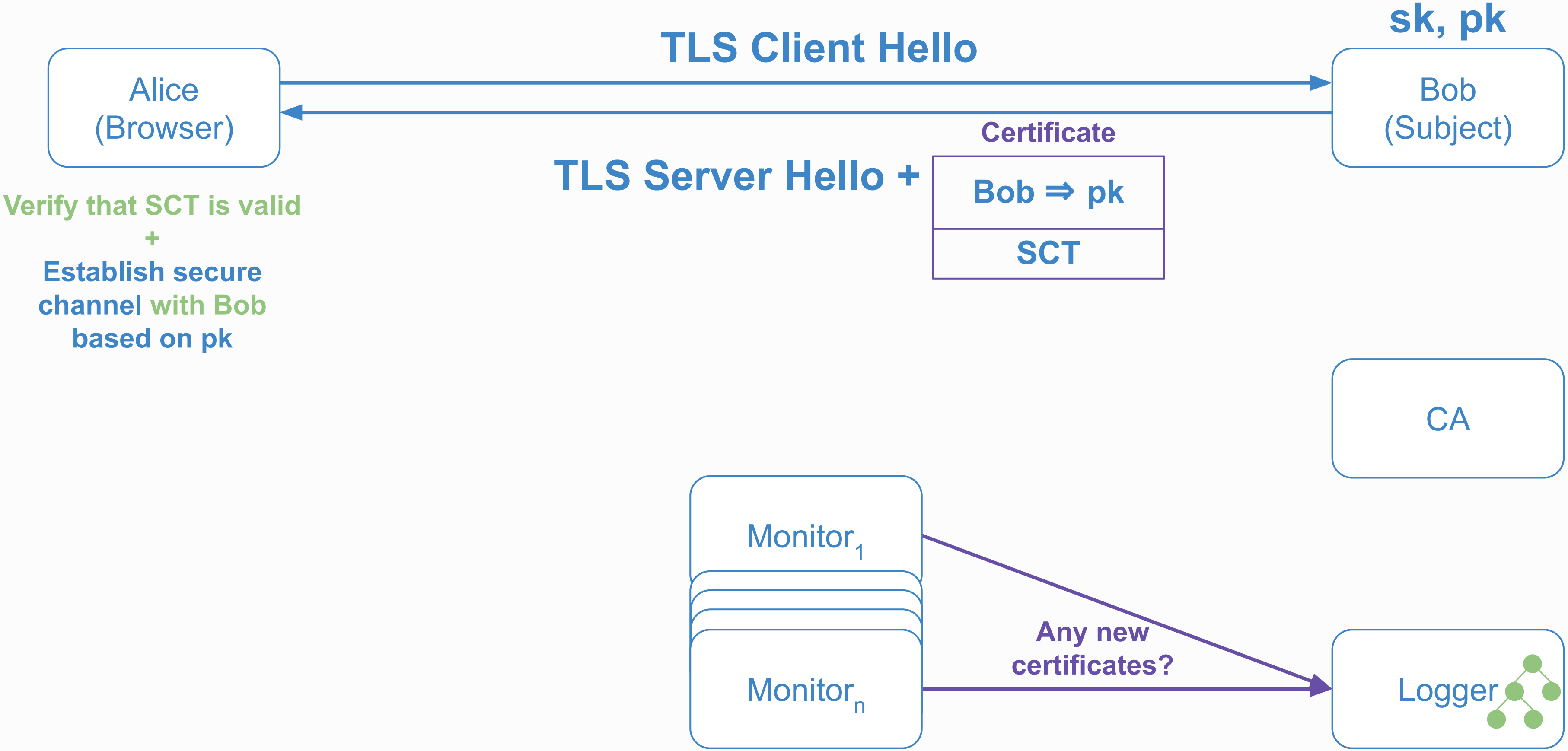
+

Establish secure channel with Bob based on pk

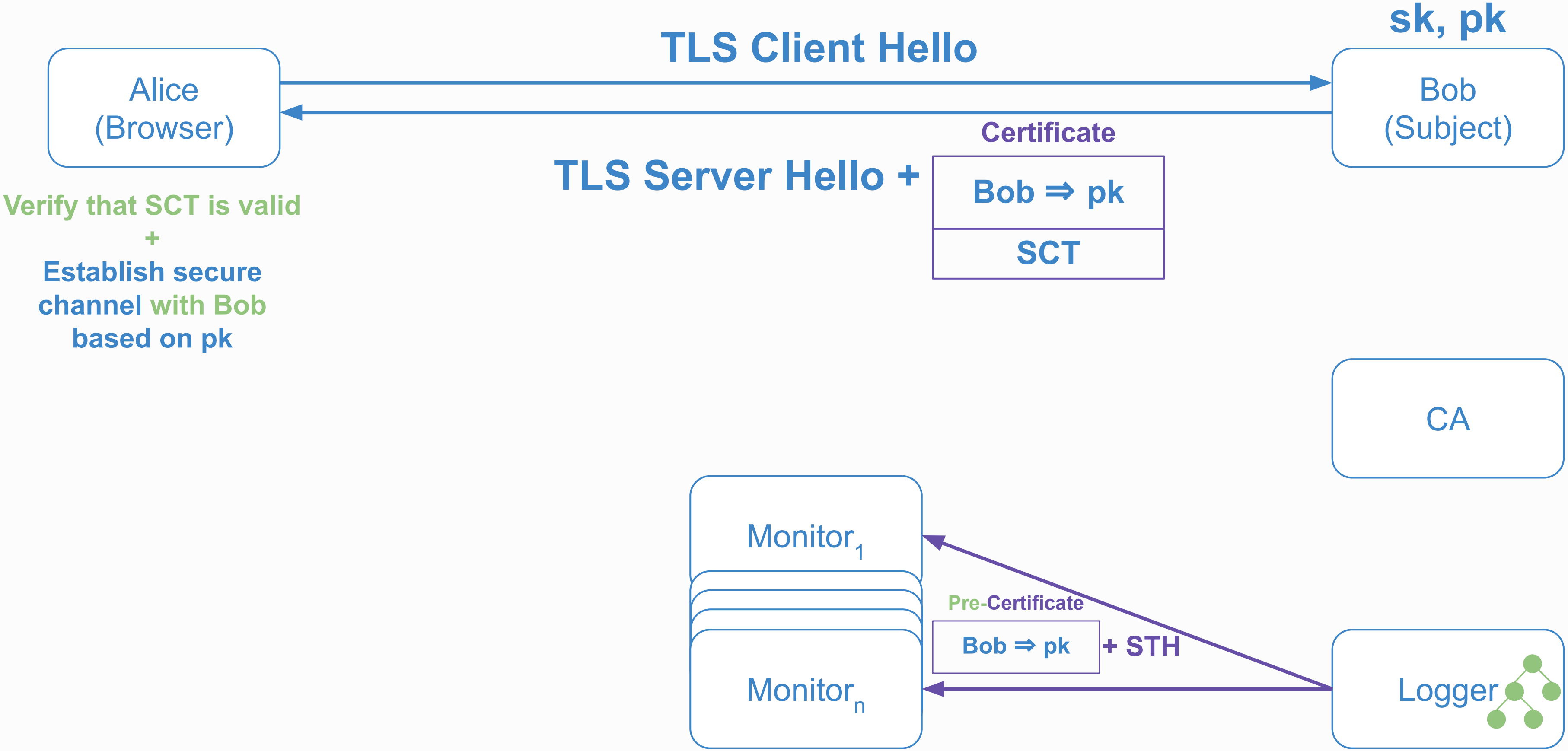
CA

Logger

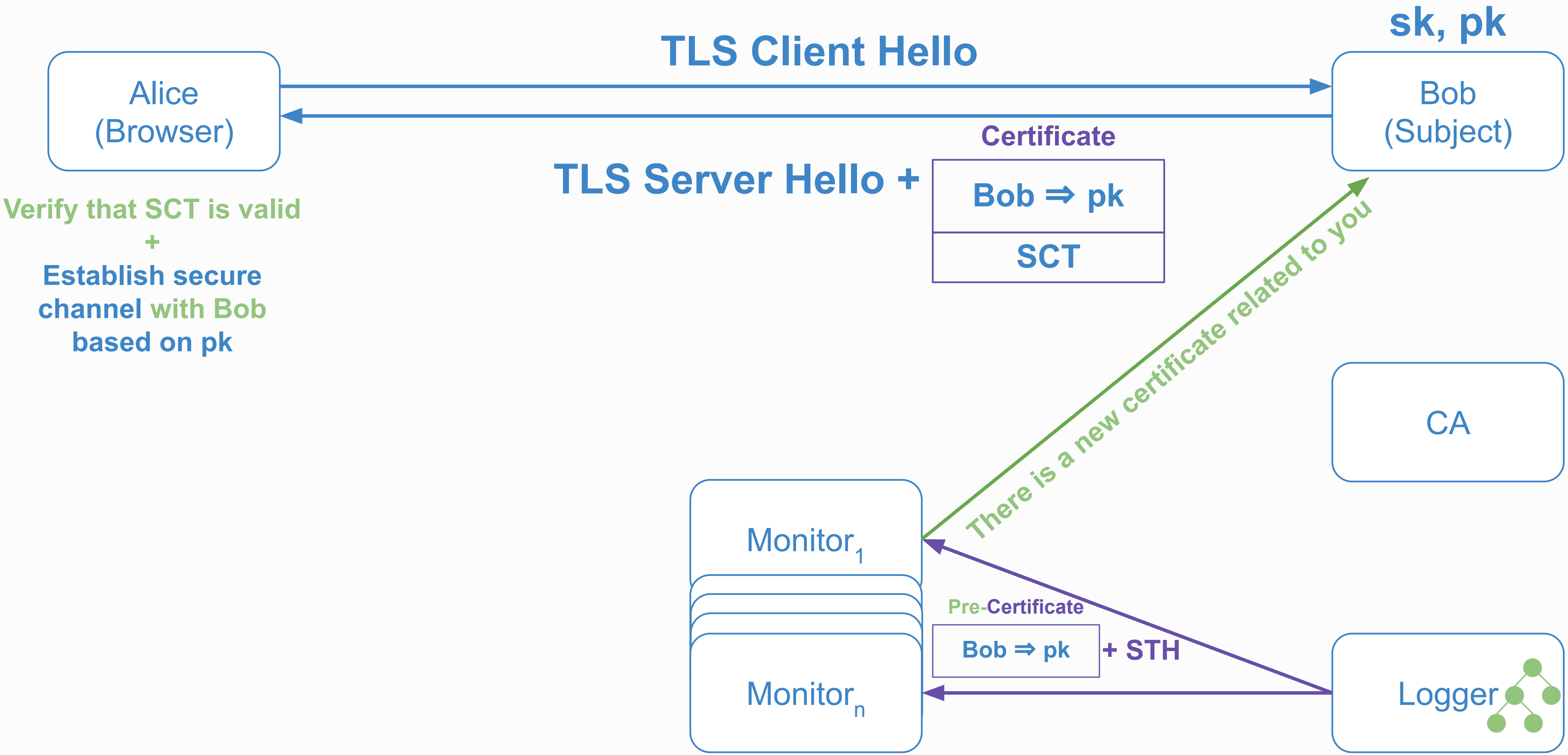
Web-PKI (X.509 + CT + Vendor-assisted revocation)



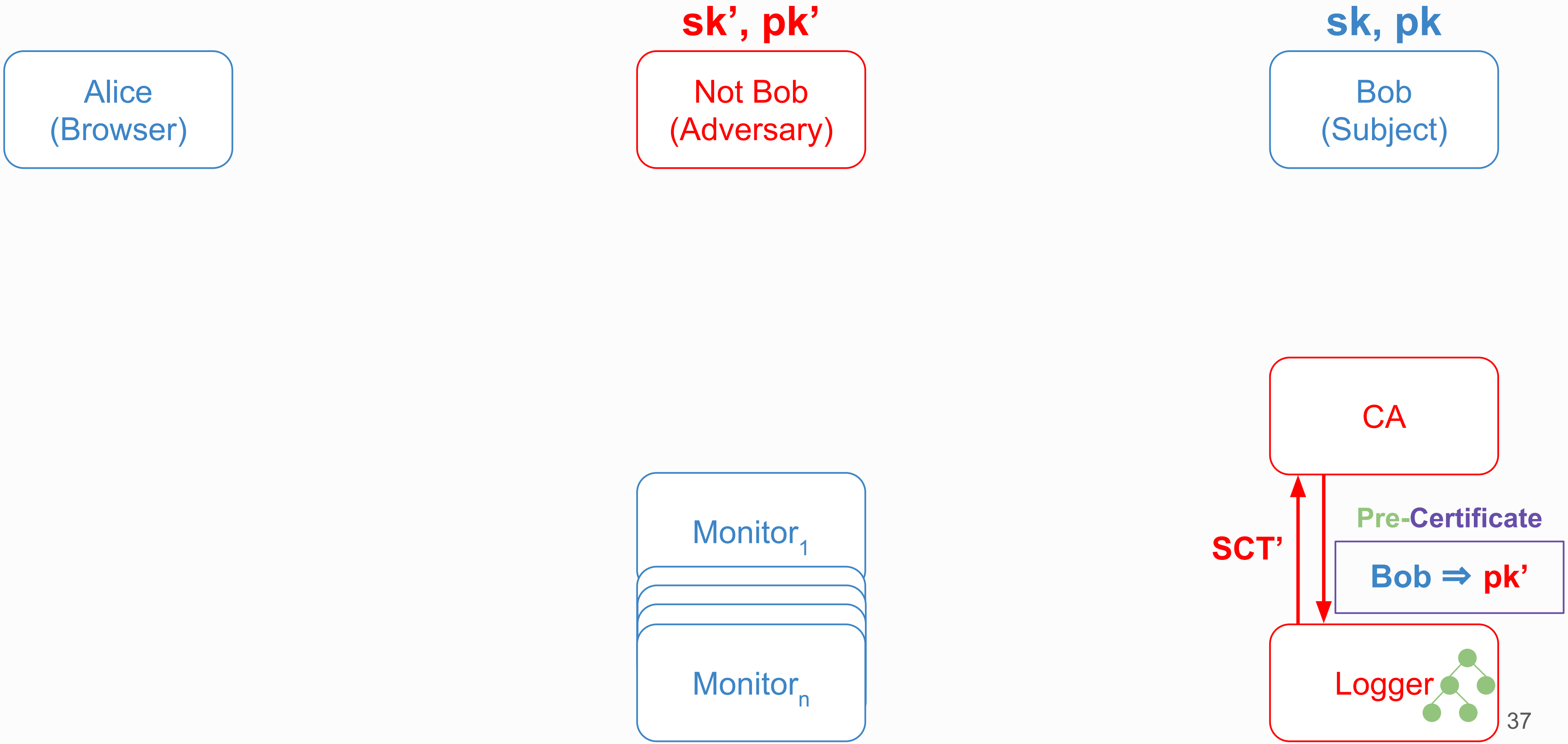
Web-PKI (X.509 + CT + Vendor-assisted revocation)



Web-PKI (X.509 + CT + Vendor-assisted revocation)



Split World Attack



sk’, pk’

sk, pk

Alice
(Browser)

Not Bob
(Adversary)

Bob
(Subject)

CA

SCT’

Pre-Certificate

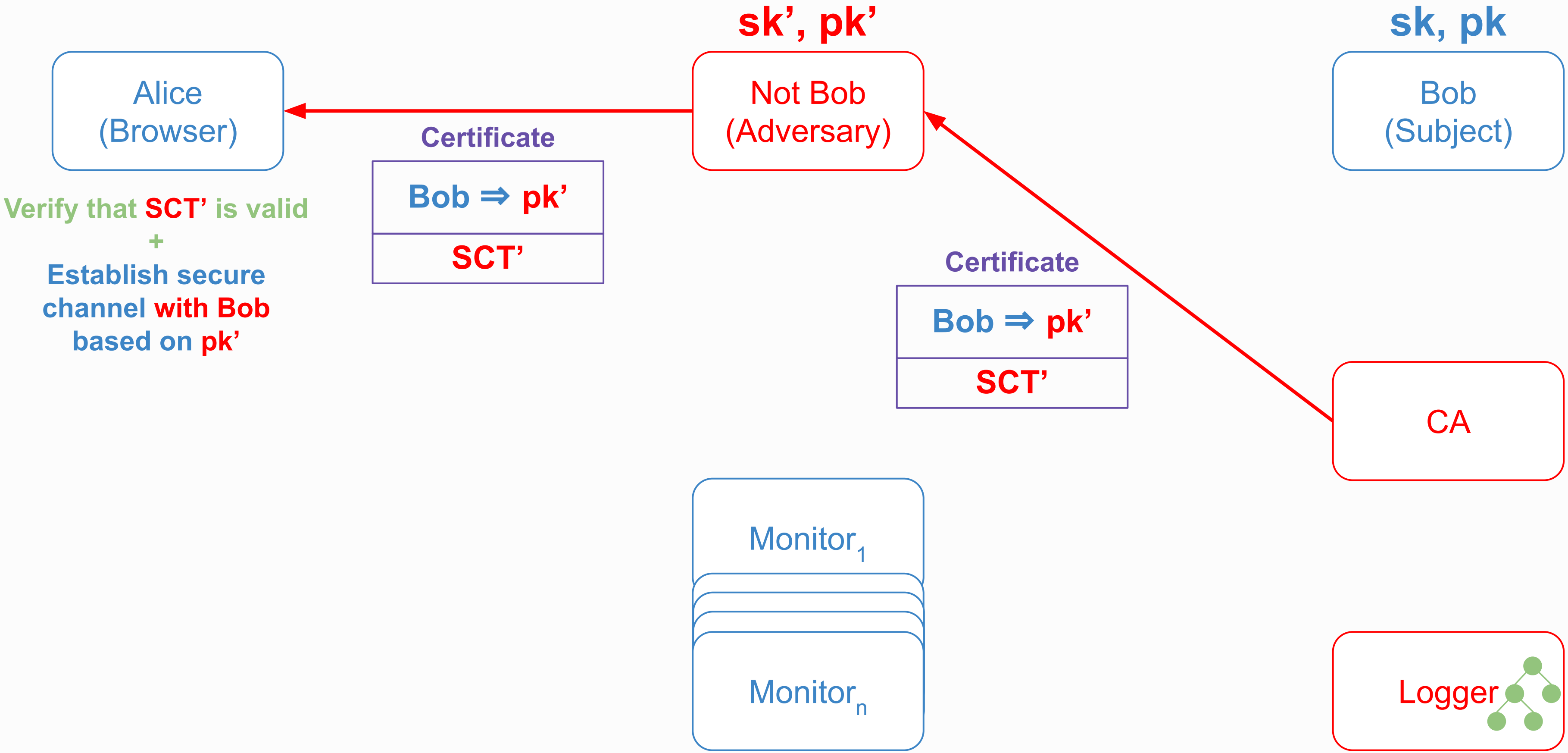
Bob ⇒ pk’

Monitor$_1$

Monitor$_n$

Logger

Split World Attack



sk', pk'

sk, pk

Alice (Browser)

Not Bob (Adversary)

Bob (Subject)

Certificate

Bob ⇒ pk'

SCT'

Verify that SCT' is valid
+
Establish secure channel with Bob based on pk'

Certificate

Bob ⇒ pk'

SCT'

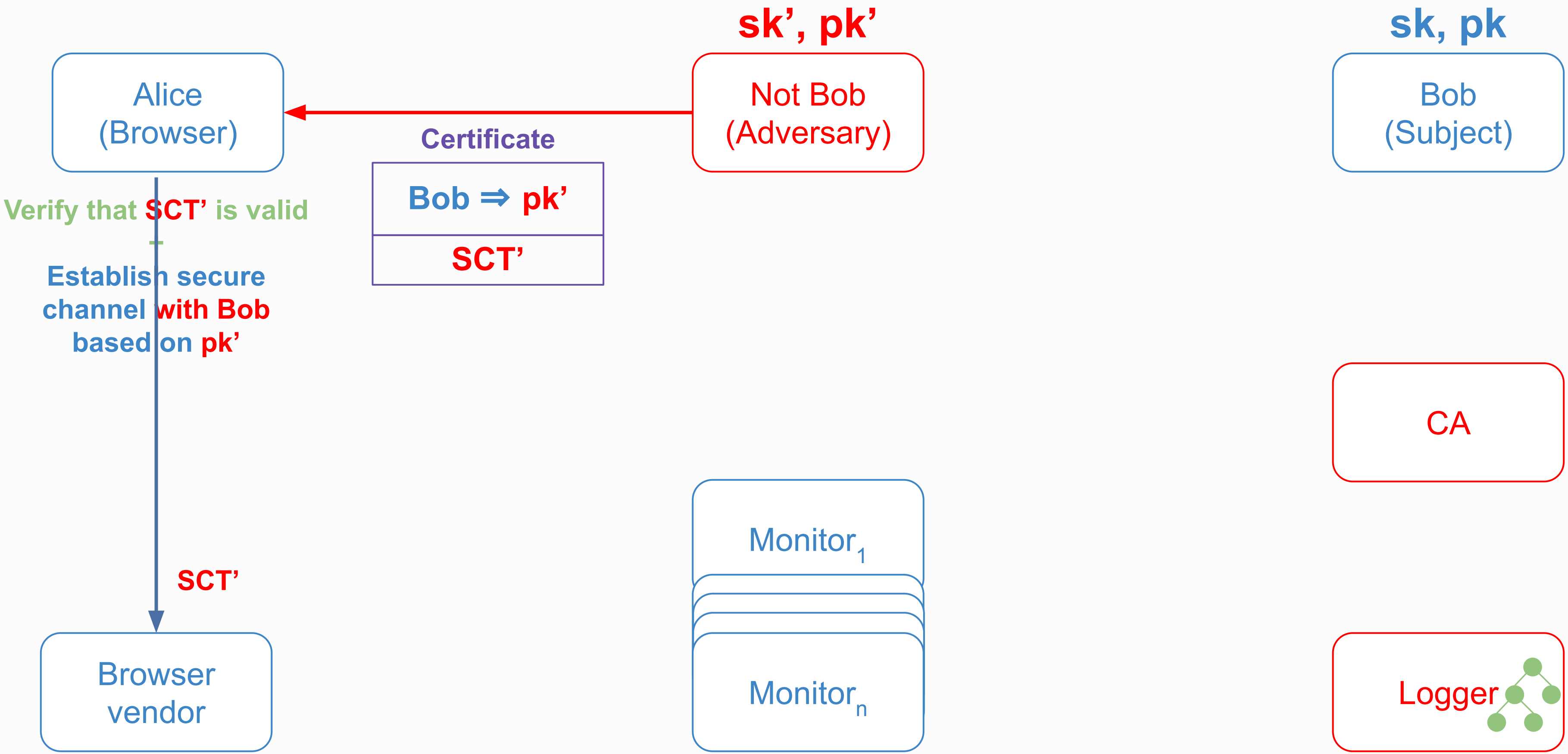
CA

Monitor$_1$

Monitor$_n$

Logger

Split World Attack



sk’, pk’

sk, pk

Alice (Browser)

Not Bob (Adversary)

Bob (Subject)

Certificate

Bob ⇒ pk’

SCT’

Verify that SCT’ is valid

+

Establish secure channel with Bob based on pk’

SCT’

CA

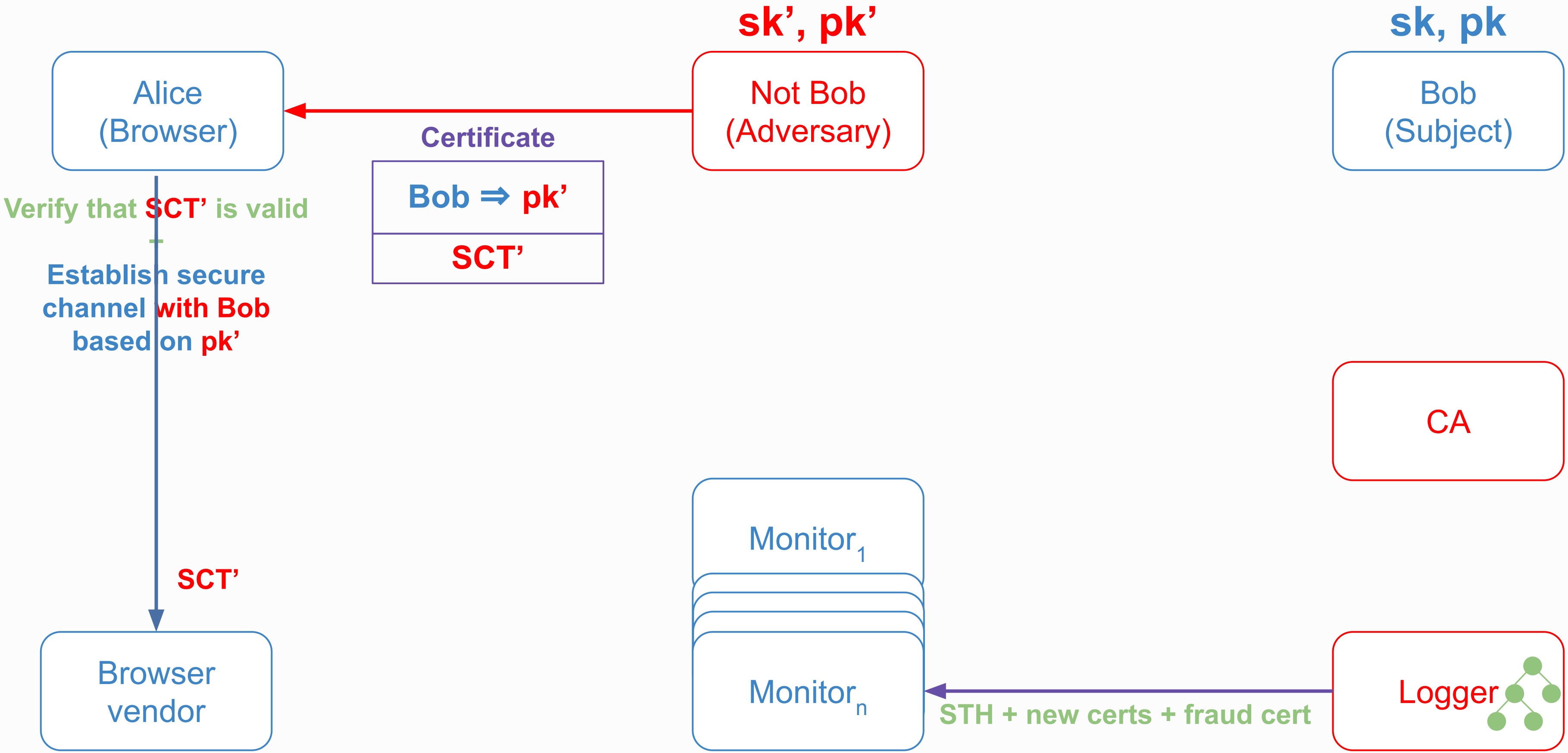
Monitor$_1$

Monitor$_n$

Browser vendor

Logger

Split World Attack



sk’, pk’

sk, pk

Alice
(Browser)

Not Bob
(Adversary)

Bob
(Subject)

Certificate

Bob ⇒ pk’

SCT’

Verify that SCT’ is valid

+

Establish secure channel with Bob based on pk’

SCT’

Browser vendor

CA

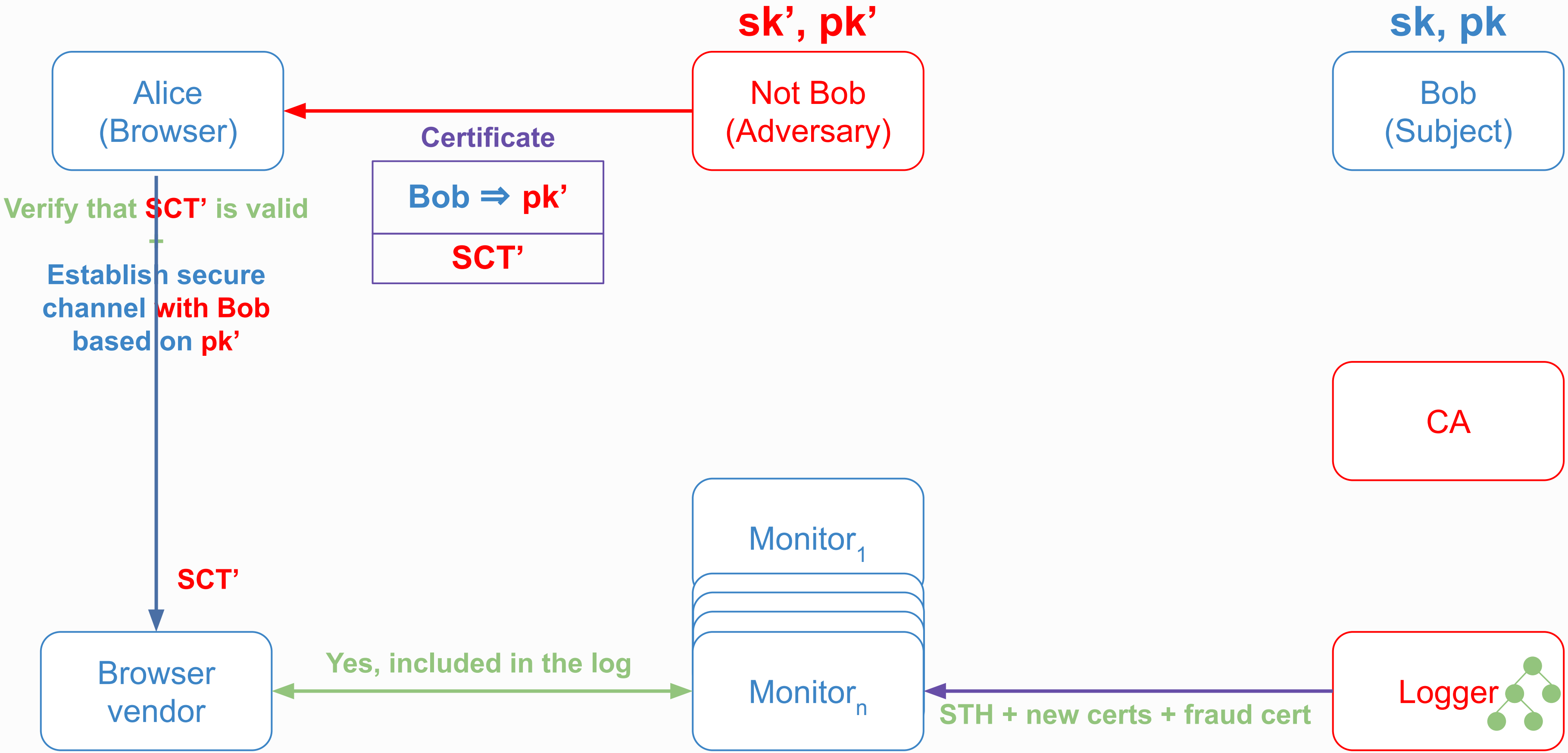
Monitor$_1$

Monitor$_n$

STH + new certs + fraud cert

Logger

Split World Attack



sk’, pk’

sk, pk

Alice
(Browser)

Not Bob
(Adversary)

Bob
(Subject)

Certificate

Bob ⇒ pk’

SCT’

Verify that SCT’ is valid
+
Establish secure channel with Bob based on pk’

CA

Monitor$_1$

SCT’

Browser vendor

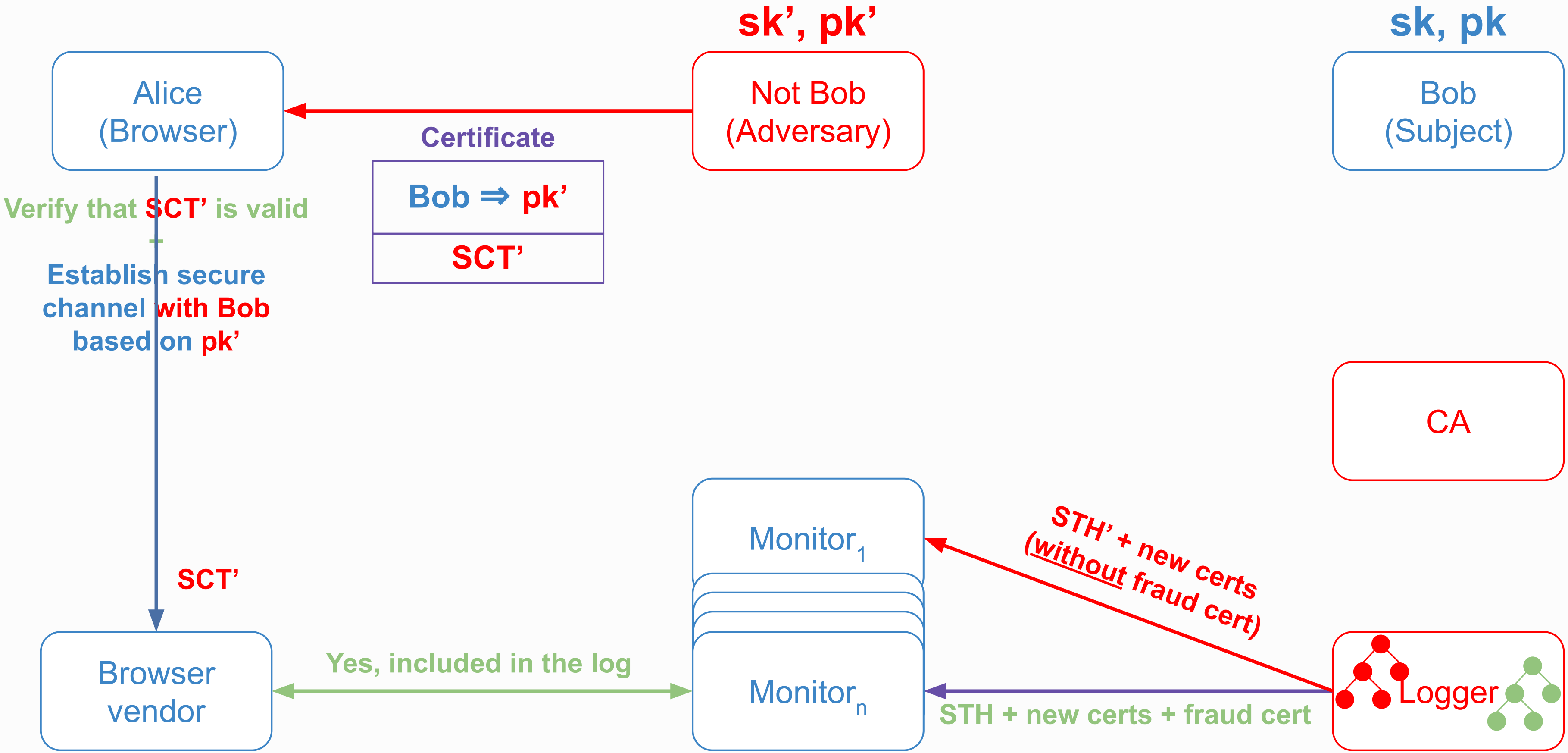
Yes, included in the log

Monitor$_n$

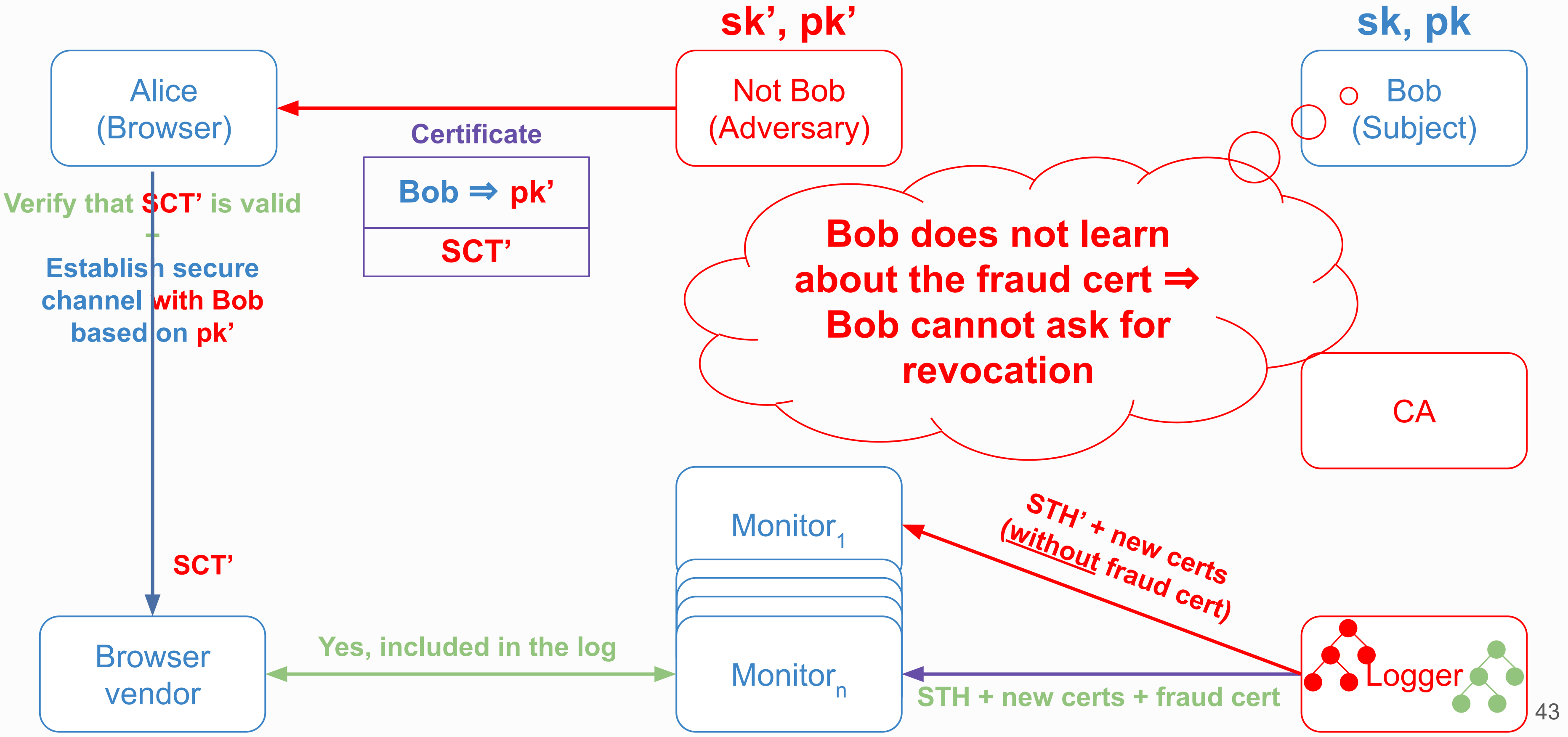
Logger

STH + new certs + fraud cert

Split World Attack

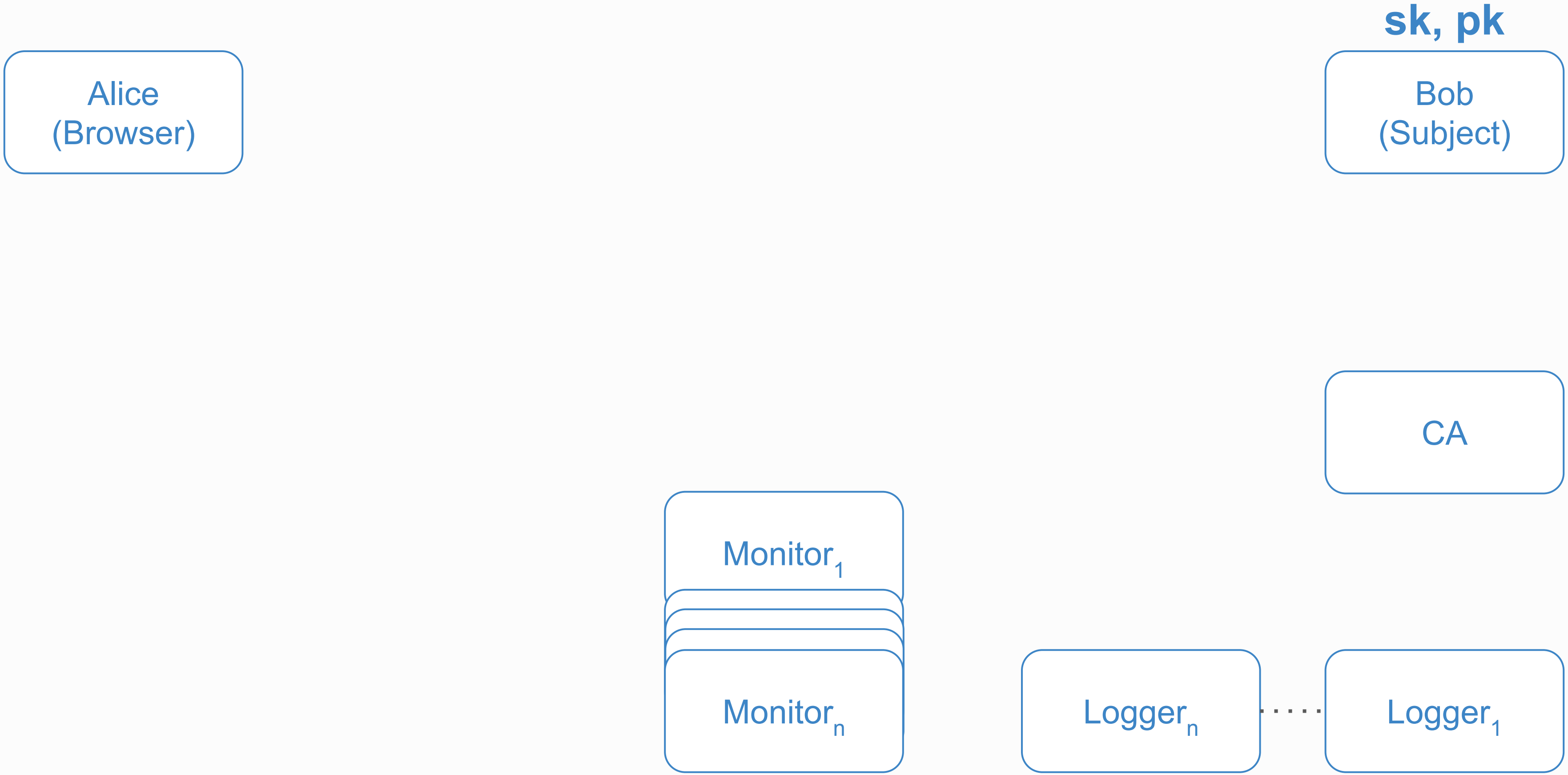


Split World Attack



sk', pk'
sk, pk
Alice (Browser)
Not Bob (Adversary)
Bob (Subject)
Certificate
Bob ⇒ pk'
SCT'
Verify that SCT' is valid
+
Establish secure channel with Bob based on pk'
Bob does not learn about the fraud cert ⇒ Bob cannot ask for revocation
CA
SCT'
Monitor$_1$
Monitor$_n$
STH' + new certs (without fraud cert)
Browser vendor
Yes, included in the log
STH + new certs + fraud cert
Logger

Log Redundancy



sk, pk

Alice (Browser)

Bob (Subject)

CA

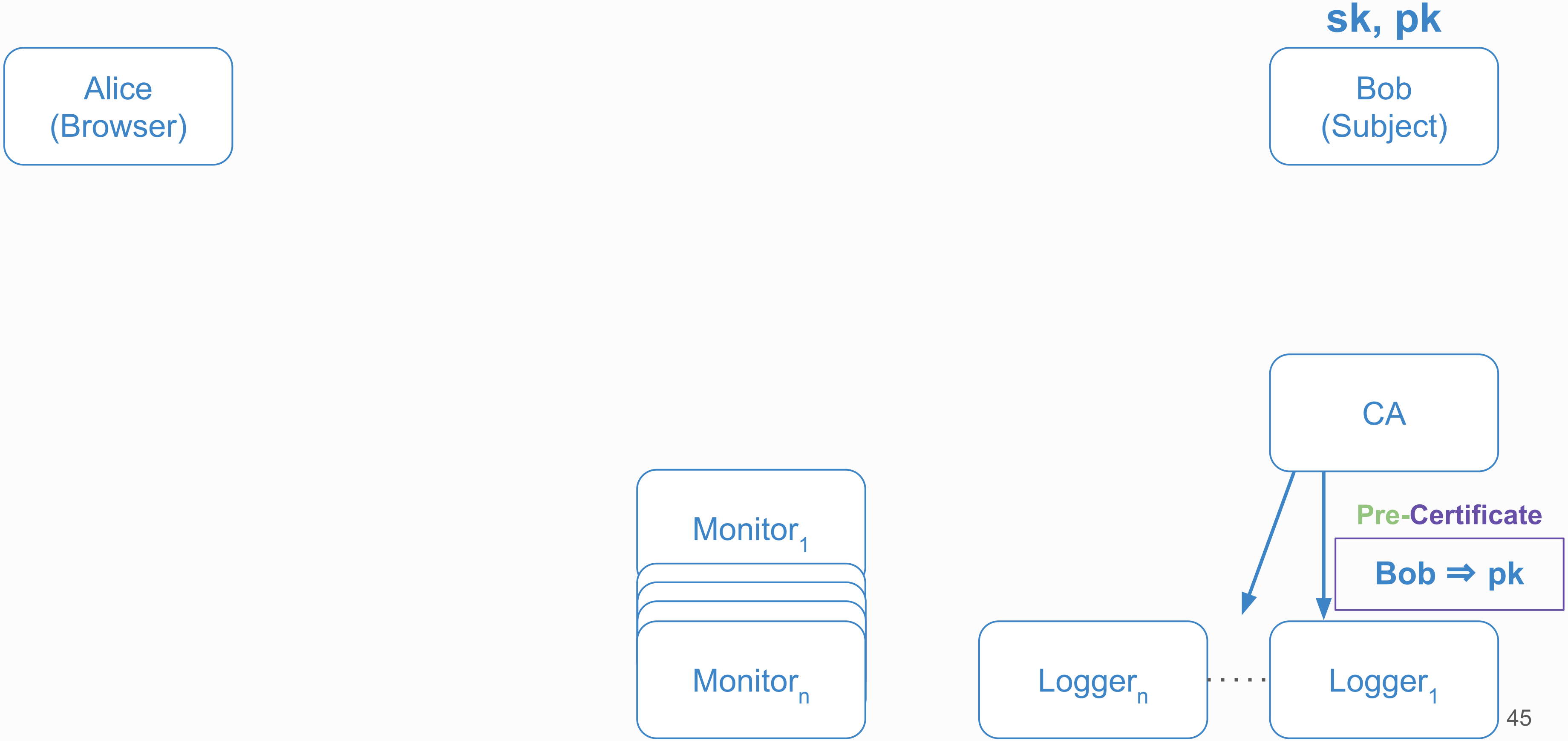
Monitor$_1$

Monitor$_n$

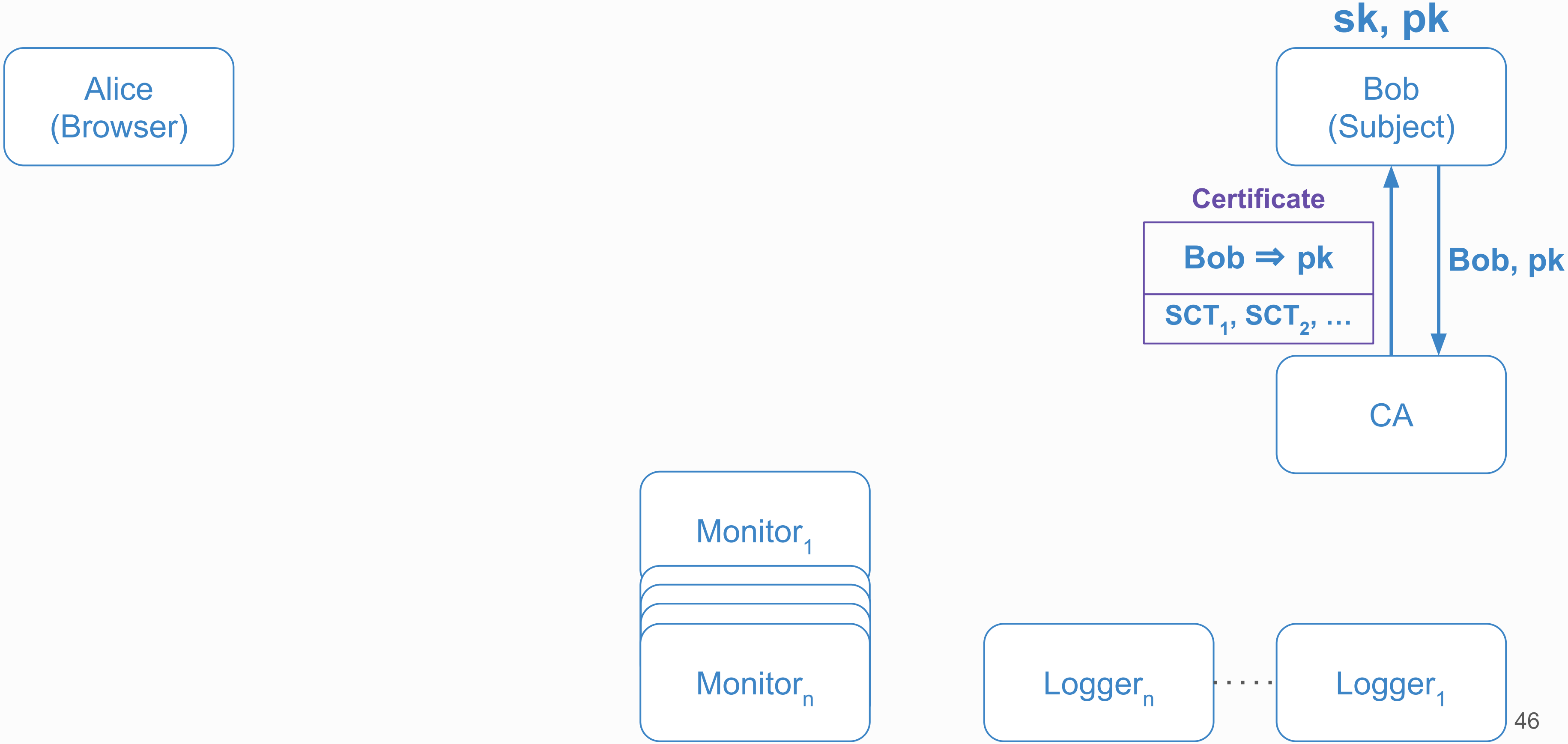
Logger$_n$

Logger$_1$

Log Redundancy



Log Redundancy



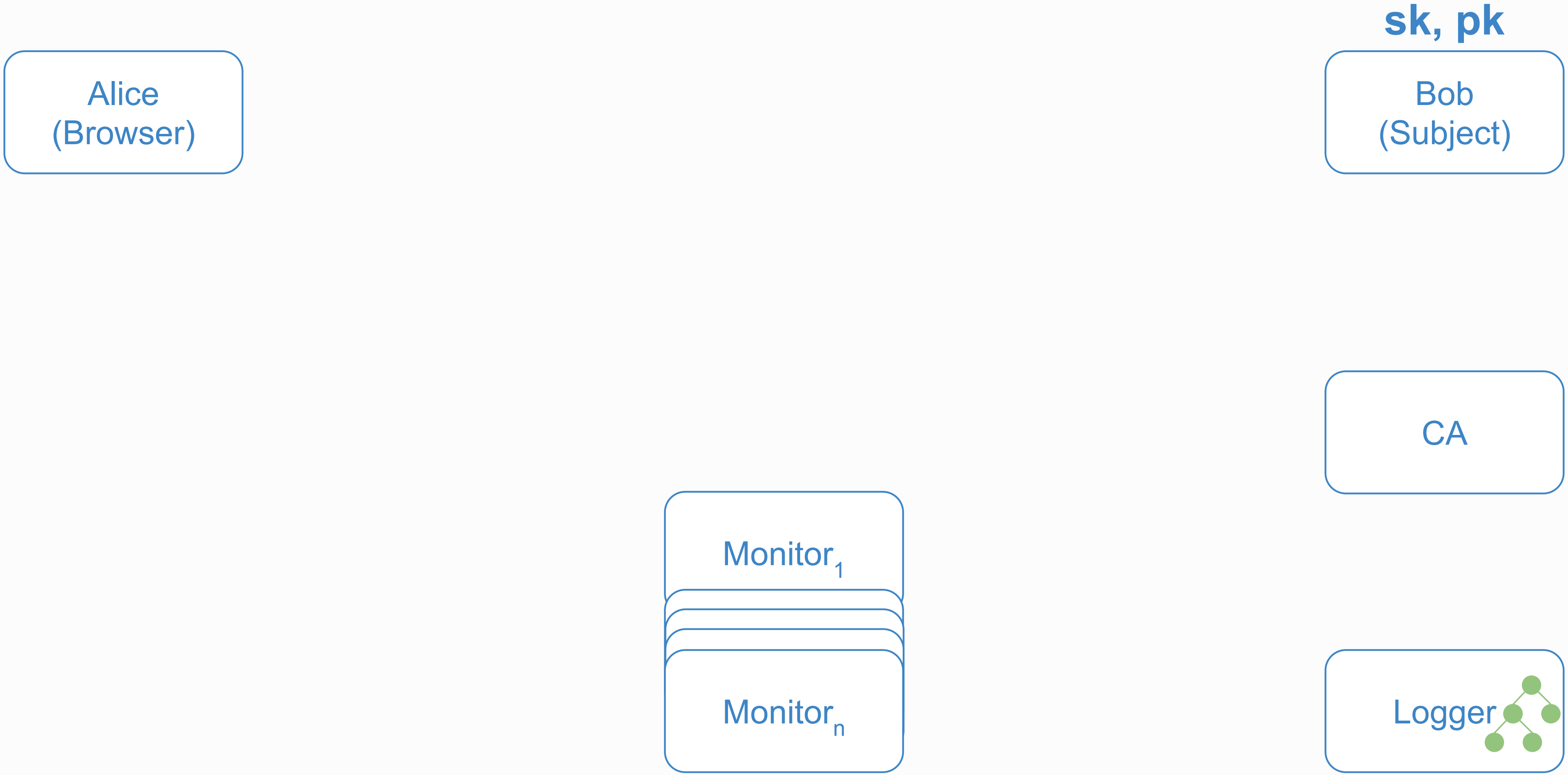
In Summary

- Revocation is broken
  - And there is no revocation transparency
- Transparency relies on log redundancy
  - Otherwise, susceptible to logger omission and split world attacks
- Relying party's efficiency and privacy issues

CTng

- An evolutionary extension
- Secure transparency and revocation
- Protecting relying parties’ privacy
- Efficient and scalable

CTng



sk, pk

Alice (Browser)

Bob (Subject)

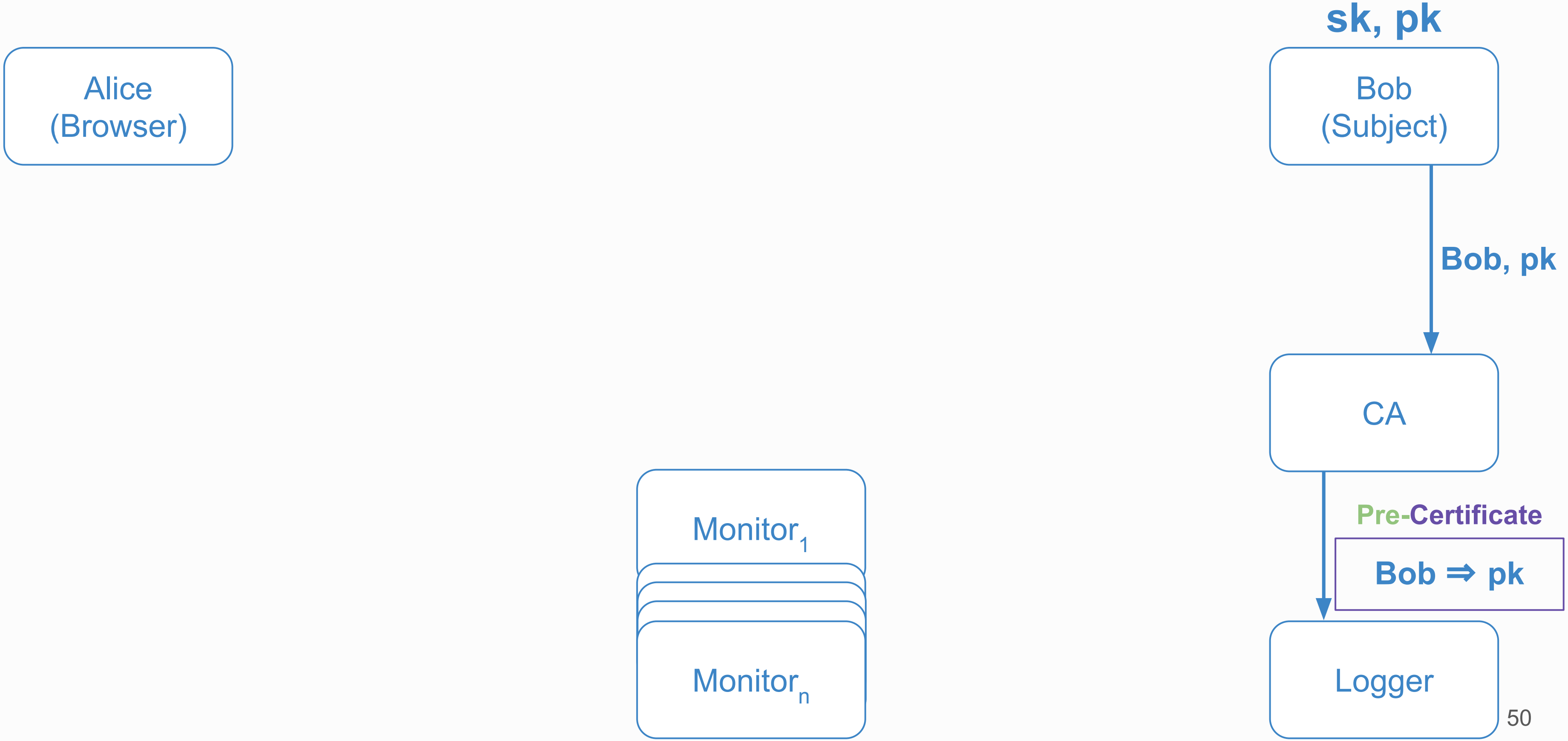
CA

Monitor$_1$

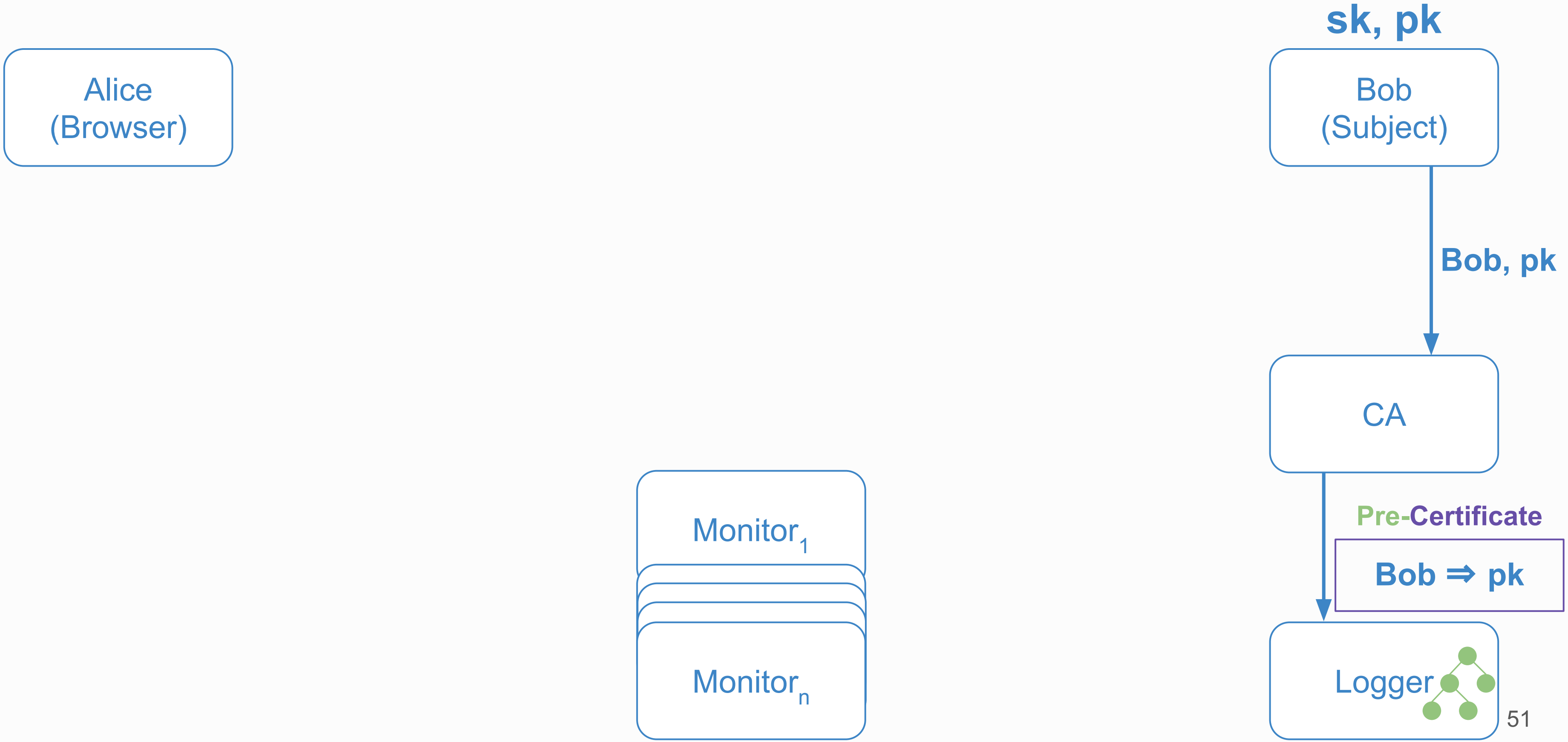
Monitor$_n$

Logger

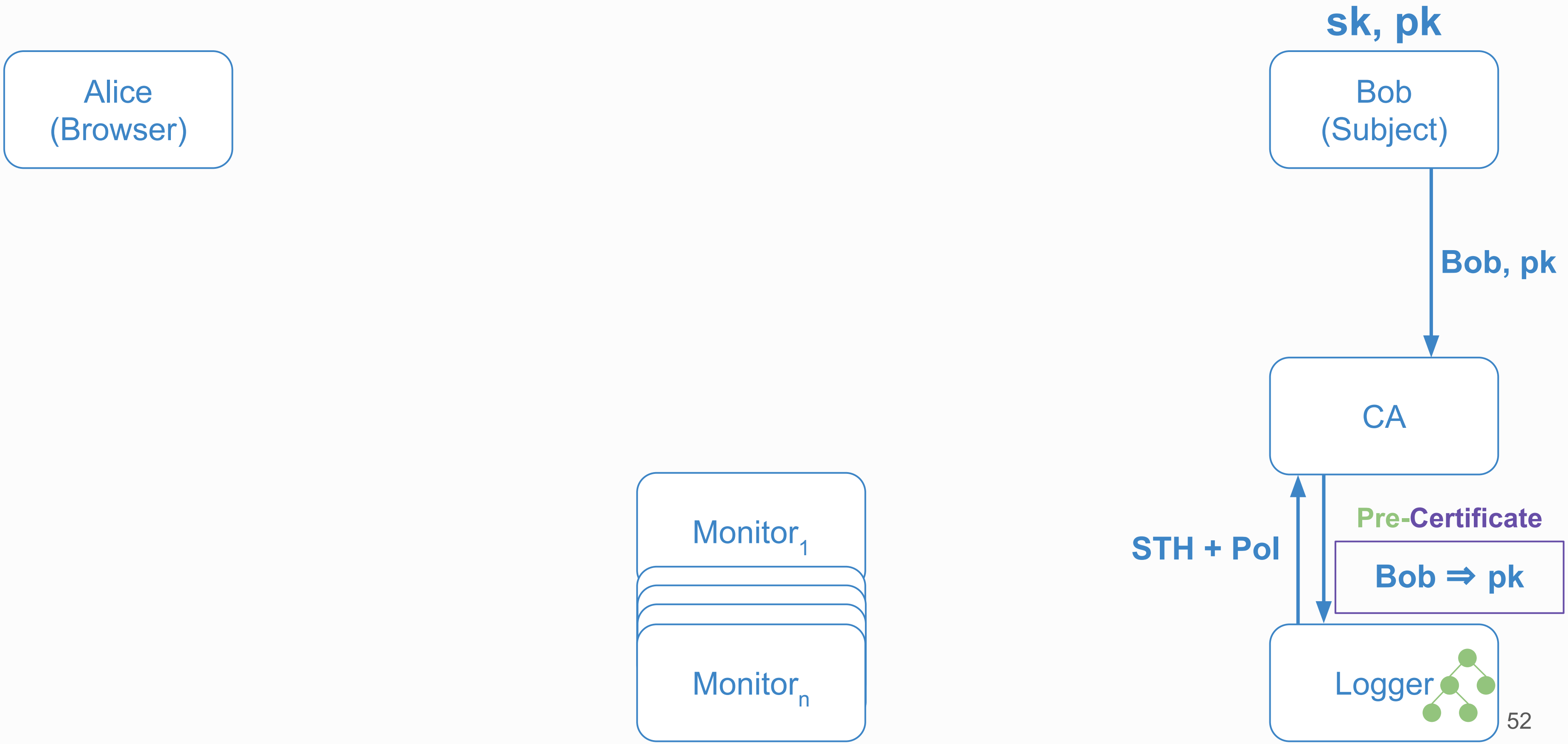
CTng


sk, pk
Alice (Browser)
Bob (Subject)
Bob, pk
CA
Pre-Certificate
Bob ⇒ pk
Monitor$_1$
Monitor$_n$
Logger

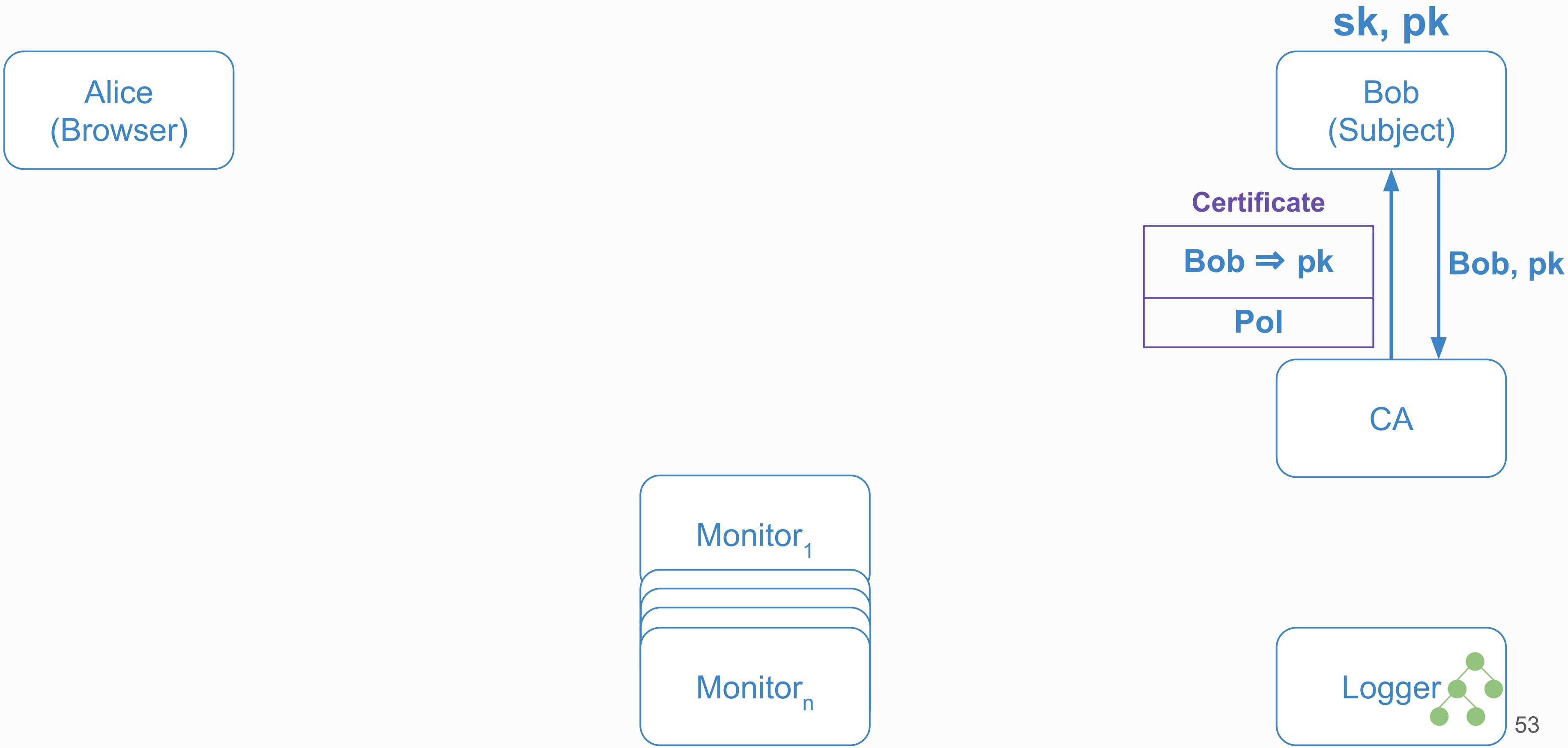
CTng


sk, pk
Alice
(Browser)
Bob
(Subject)
Bob, pk
CA
Pre-Certificate
Bob ⇒ pk
Monitor$_1$
Monitor$_n$
Logger

CTng


sk, pk
Alice
(Browser)
Bob
(Subject)
Bob, pk
CA
Pre-Certificate
Bob ⇒ pk
STH + PoI
Monitor$_1$
Monitor$_n$
Logger

CTng



sk, pk

Alice
(Browser)

Bob
(Subject)

Certificate

Bob ⇒ pk

PoI

Bob, pk

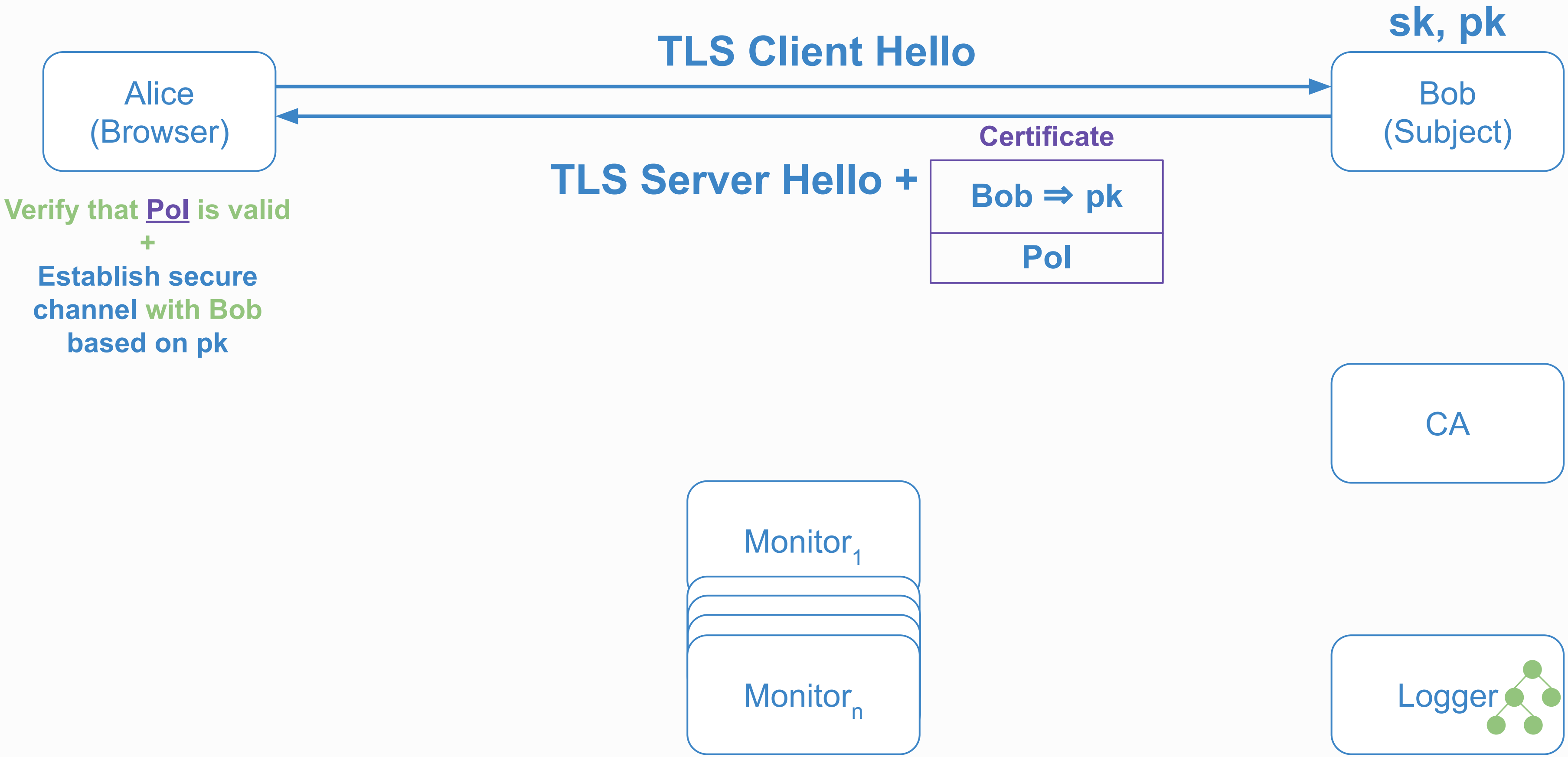
CA

Monitor$_1$

Monitor$_n$

Logger

CTng



sk, pk

TLS Client Hello

Alice (Browser)

Bob (Subject)

TLS Server Hello +

Certificate

Bob ⇒ pk

PoI

Verify that PoI is valid
+
Establish secure channel with Bob based on pk

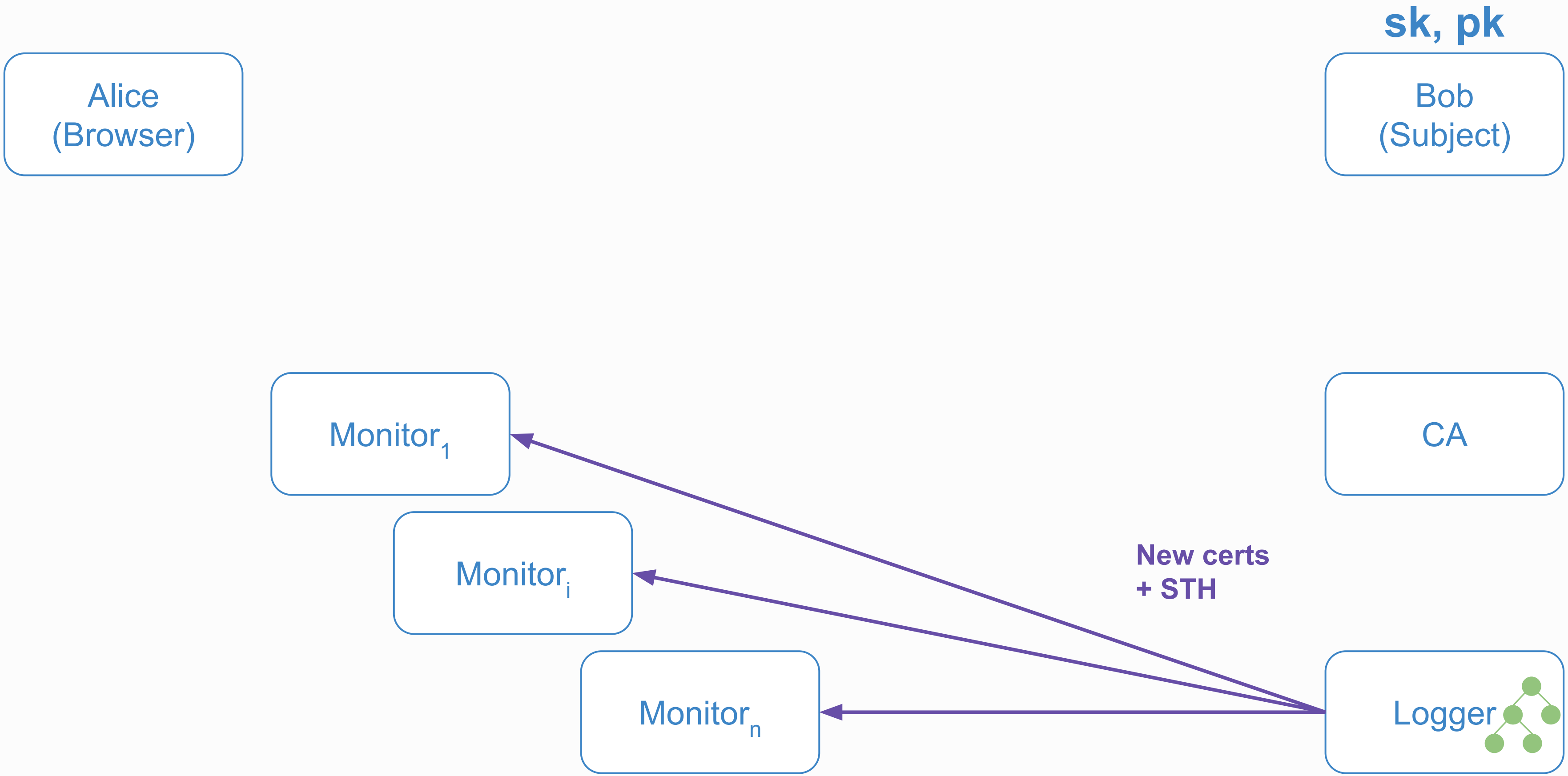
CA

Monitor_1

Monitor_n

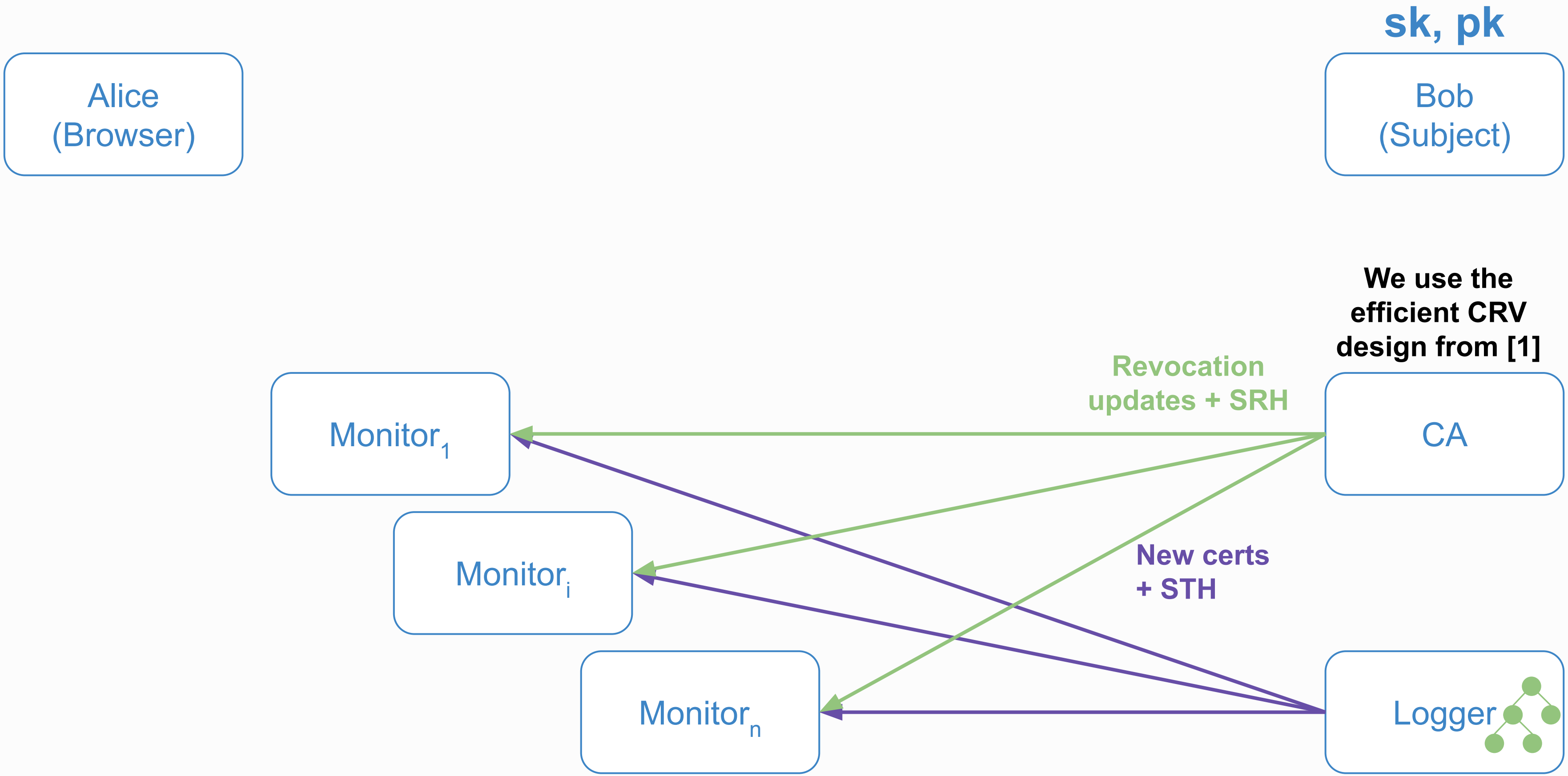
Logger

CTng


sk, pk
Alice (Browser)
Bob (Subject)
Monitor$_1$
CA
New certs + STH
Monitor$_i$
Monitor$_n$
Logger

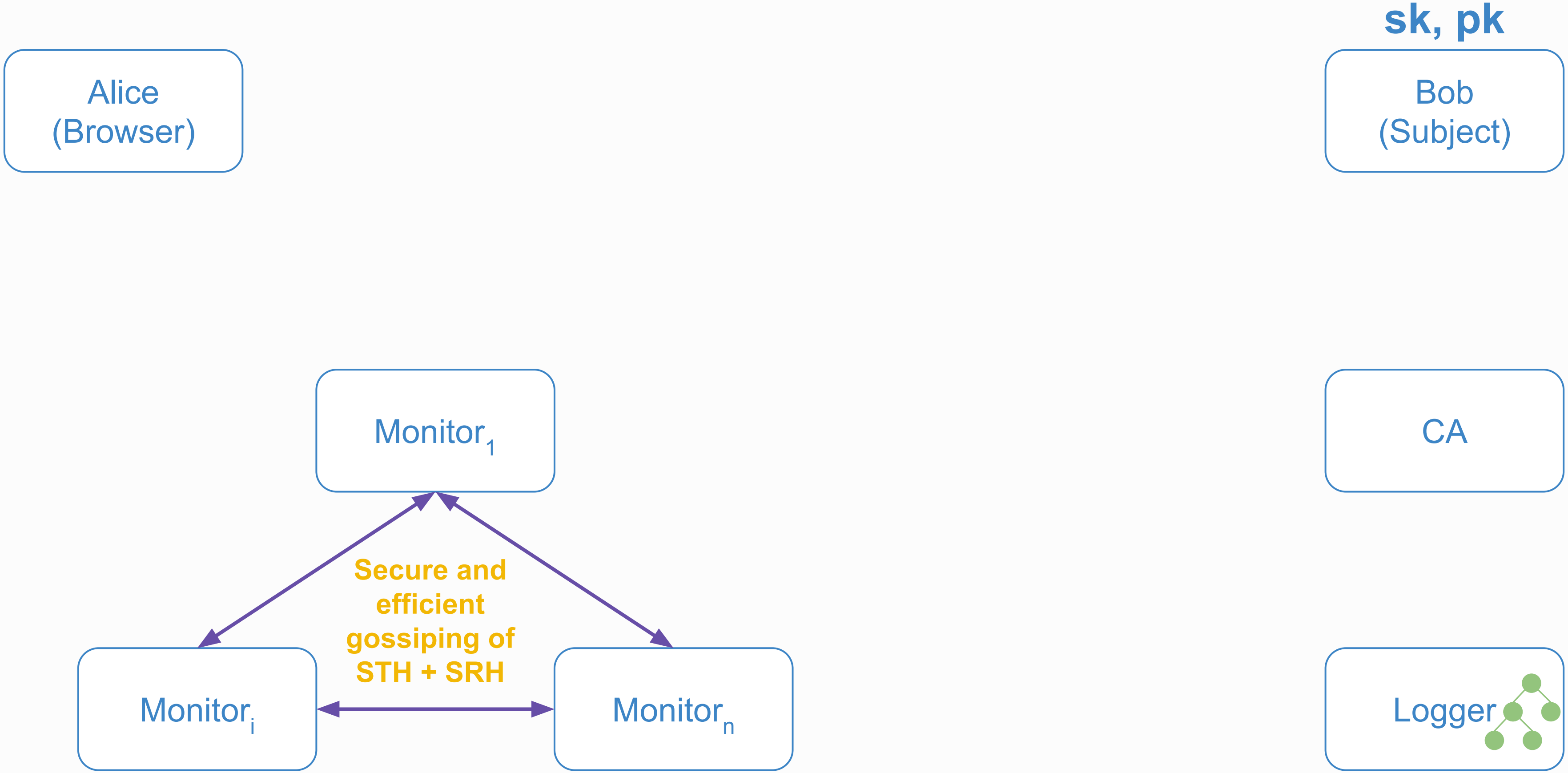
CTng

[1] Smith, Trevor, Luke Dickinson, and Kent Seamons. "Let's revoke: Scalable global certificate revocation." *Network and Distributed Systems Security (NDSS) Symposium 2020*. 2020.



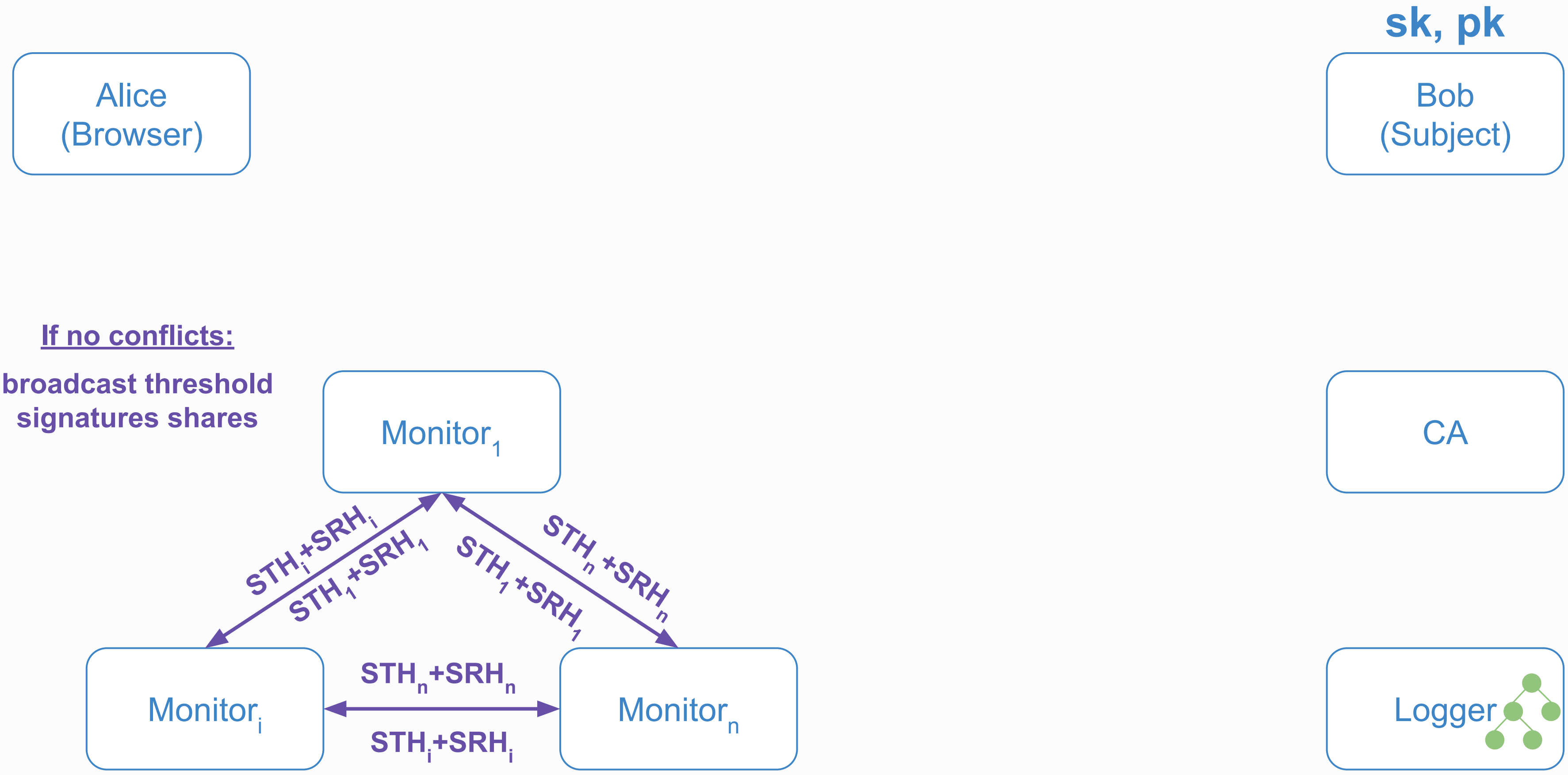
We use the efficient CRV design from [1]

CTng



sk, pk
Alice (Browser)
Bob (Subject)
Monitor$_1$
CA
Secure and efficient gossiping of STH + SRH
Monitor$_i$
Monitor$_n$
Logger

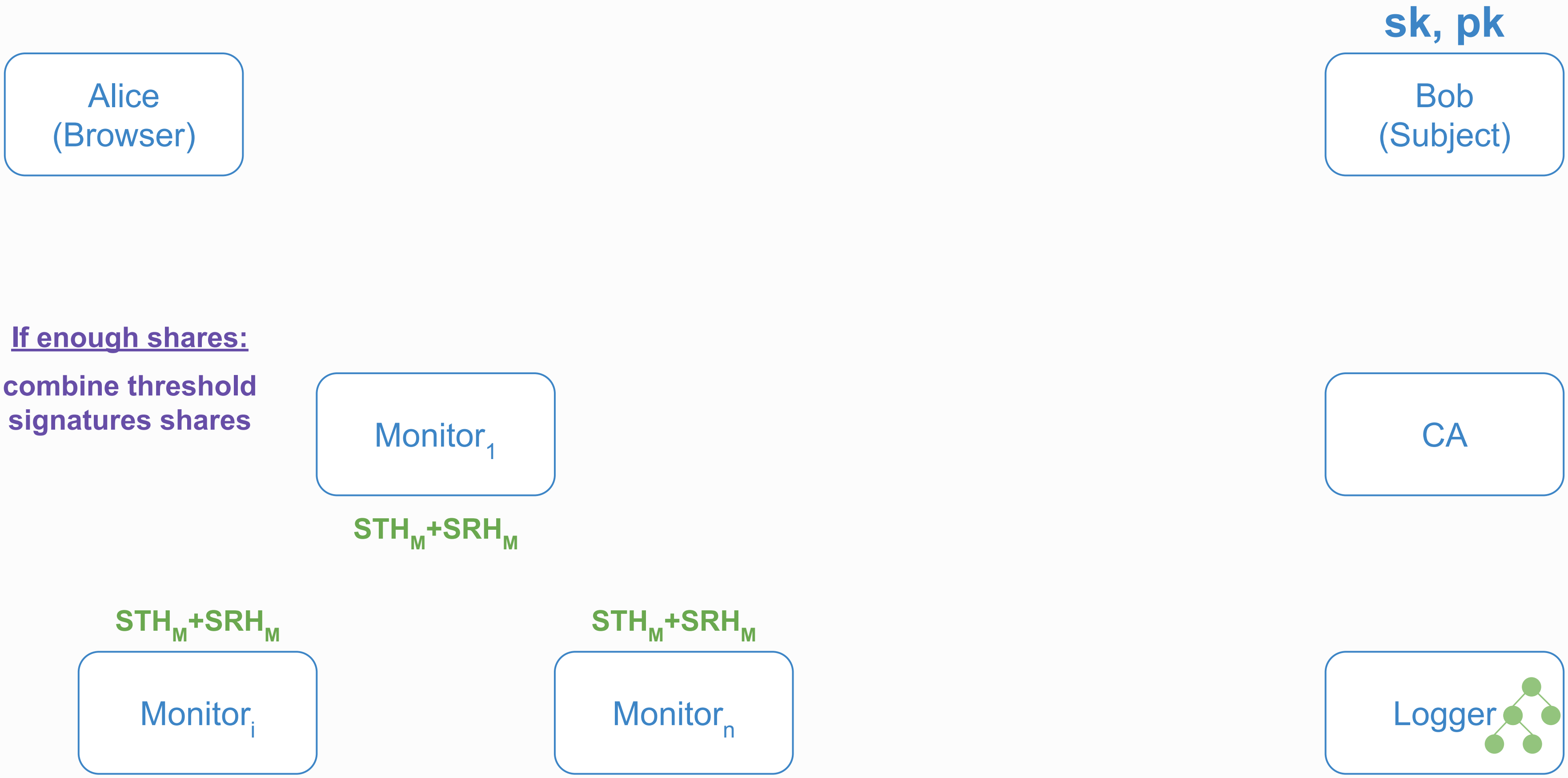
CTng



If no conflicts:

broadcast threshold signatures shares

CTng



sk, pk

Alice
(Browser)

Bob
(Subject)

<u>If enough shares:</u>

combine threshold signatures shares

Monitor_1

CA

$\text{STH}_M\text{+SRH}_M$

$\text{STH}_M\text{+SRH}_M$

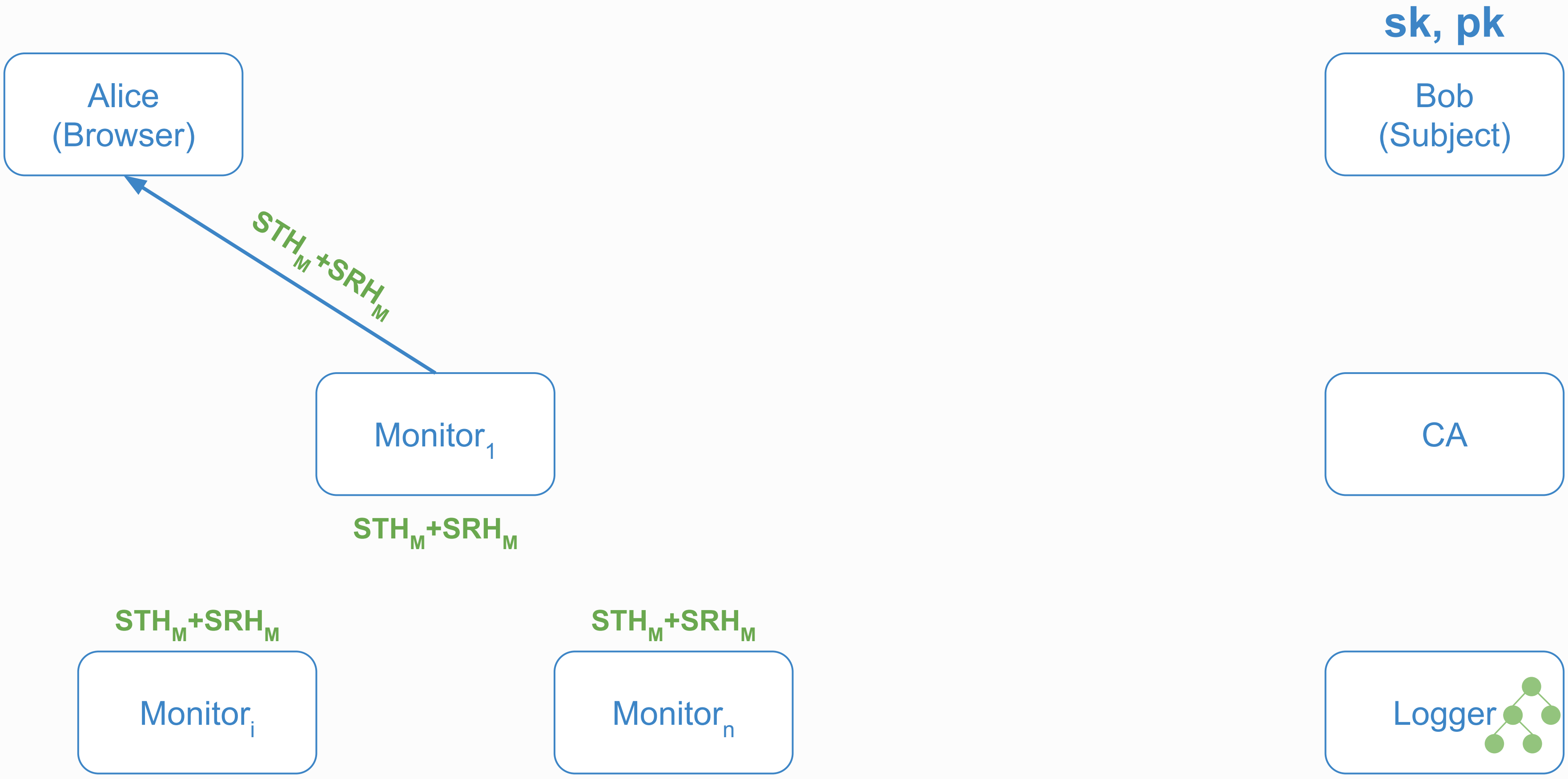
$\text{STH}_M\text{+SRH}_M$

Monitor_i

Monitor_n

Logger

CTng



sk, pk

Alice (Browser)

Bob (Subject)

STH_M+SRH_M

Monitor$_1$

CA

STH_M+SRH_M

STH_M+SRH_M

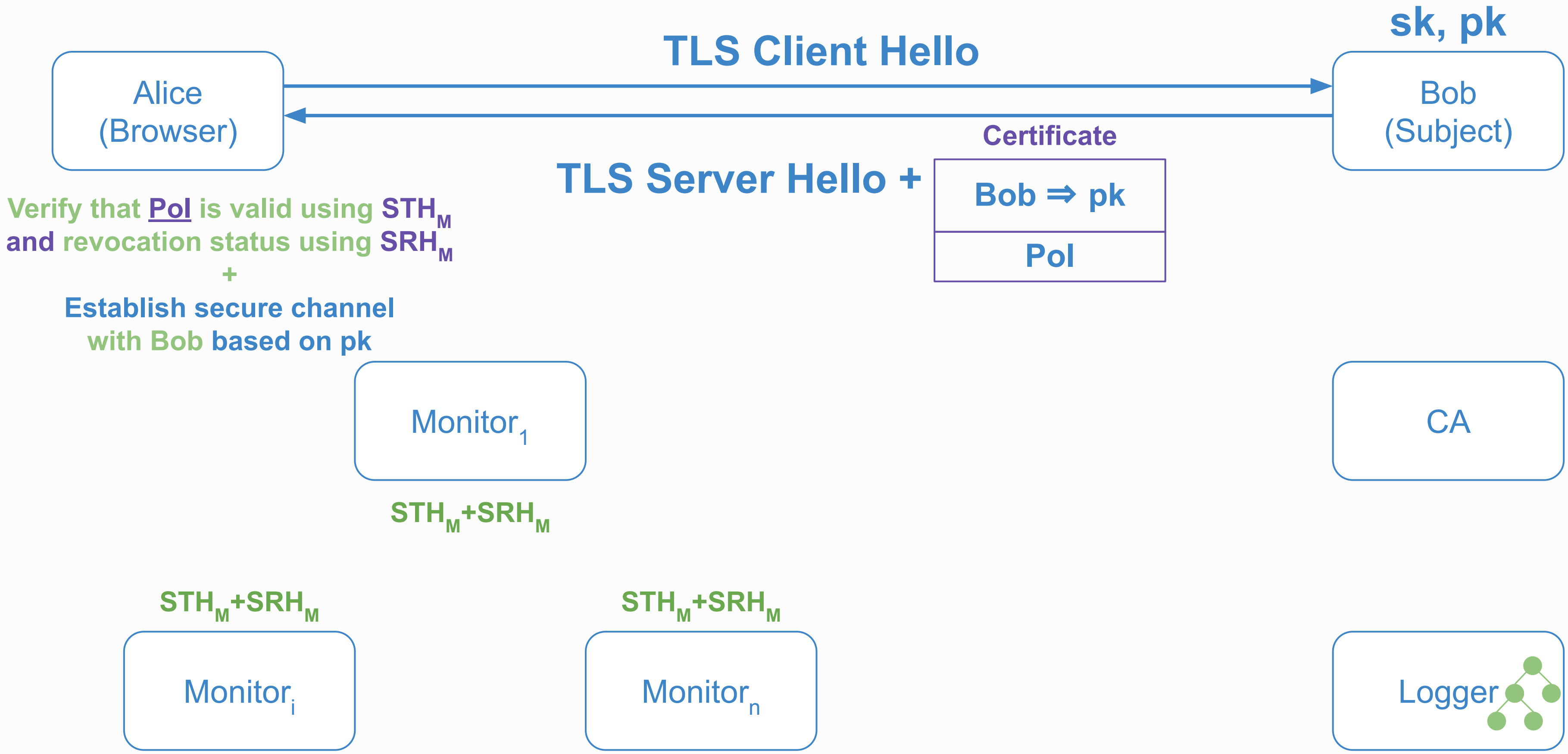
STH_M+SRH_M

Monitor$_i$

Monitor$_n$

Logger

CTng



sk, pk

TLS Client Hello

Alice (Browser)

Bob (Subject)

TLS Server Hello +

Certificate

Bob ⇒ pk

PoI

Verify that PoI is valid using STH_M and revocation status using SRH_M
+
Establish secure channel with Bob based on pk

Monitor$_1$

STH_M+SRH_M

CA

STH_M+SRH_M

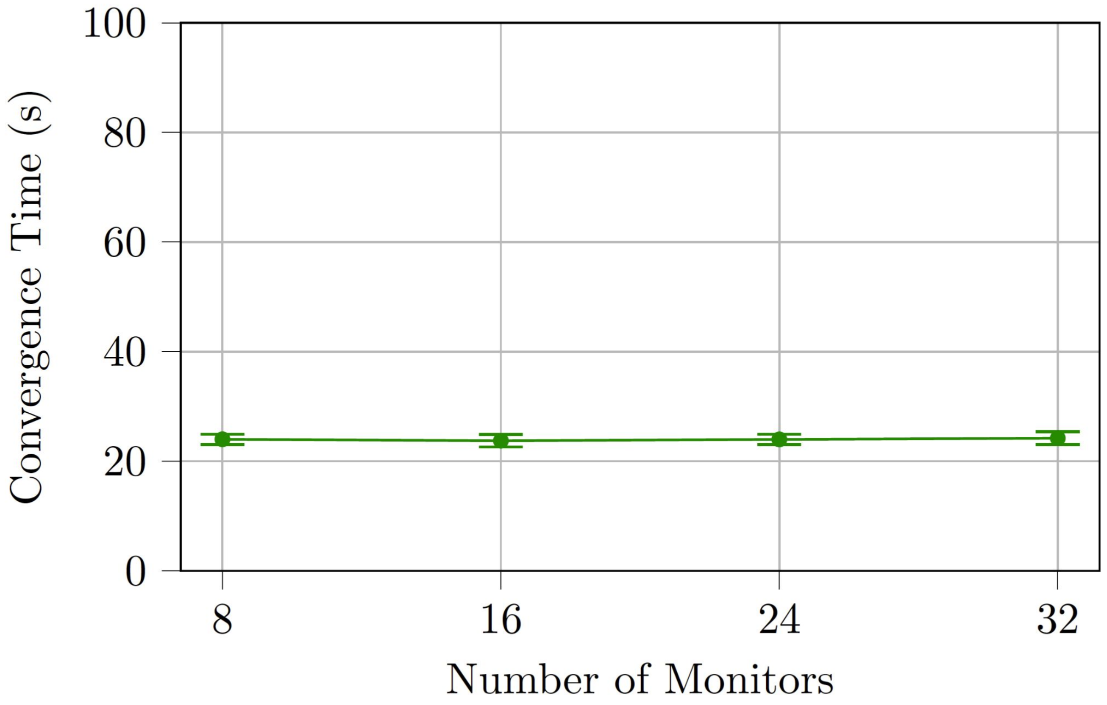
STH_M+SRH_M

Monitor$_i$

Monitor$_n$

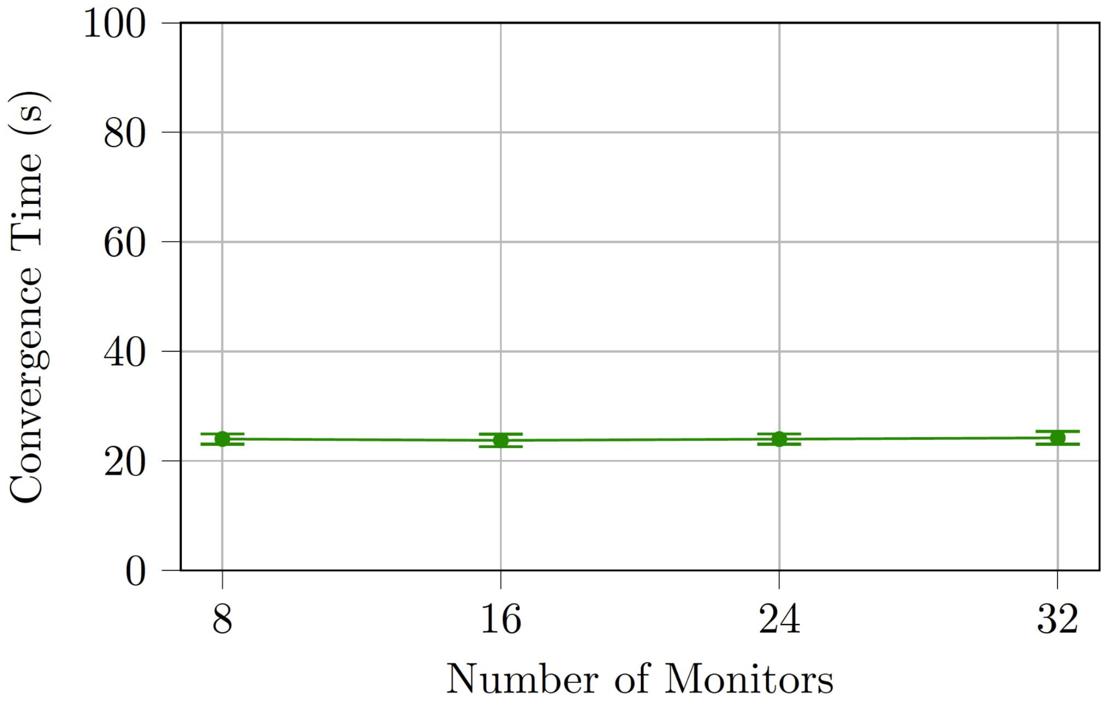
Logger

CTng Evaluation (Varying number of monitors)



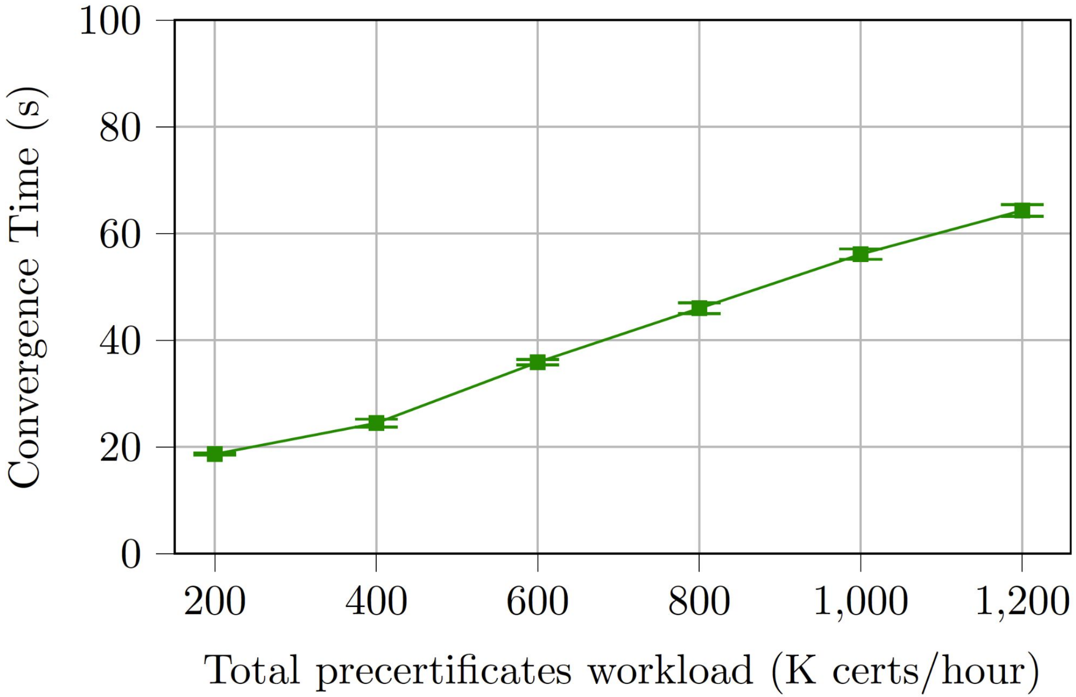
# of monitors in CT (as of 1/2025): 6 orgs, each running 1–3 logs

CTng Evaluation (Varying number of monitors)



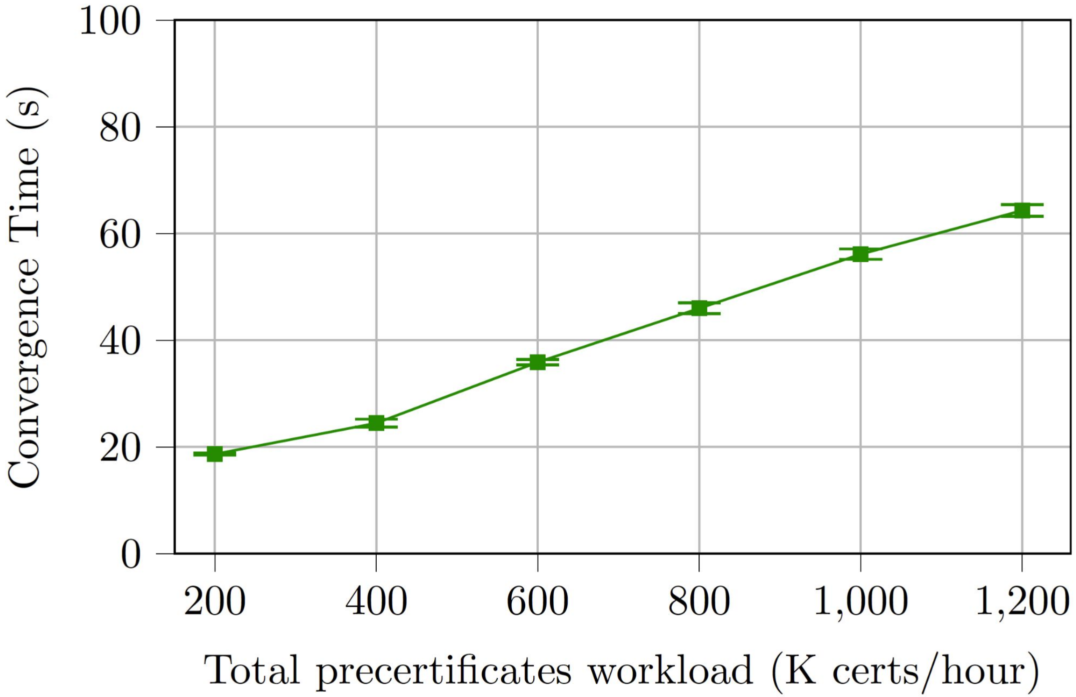
The convergence time of CTng does not significantly increase due to an increase in the number of monitors

CTng Evaluation (Different total precertificates workload)



# of unique certificates/hr (during 12/2024): ~400K

CTng Evaluation (Different total precertificates workload)



CTng scales linearly with the input workload and can support MMDs in the order of minutes

Conclusions

- We presented CTng:
    - An evolutionary extension of CT and the current Web-PKI
    - Secure transparency and revocation
    - Protects relying parties’ privacy
    - Efficient and scalable

Thank you!

Any questions?