Securing dCache Communications

Anupam Ashish, on behalf of dCache team

11th International dCache Workshop 2017, Umea, Sweden

Fermilab

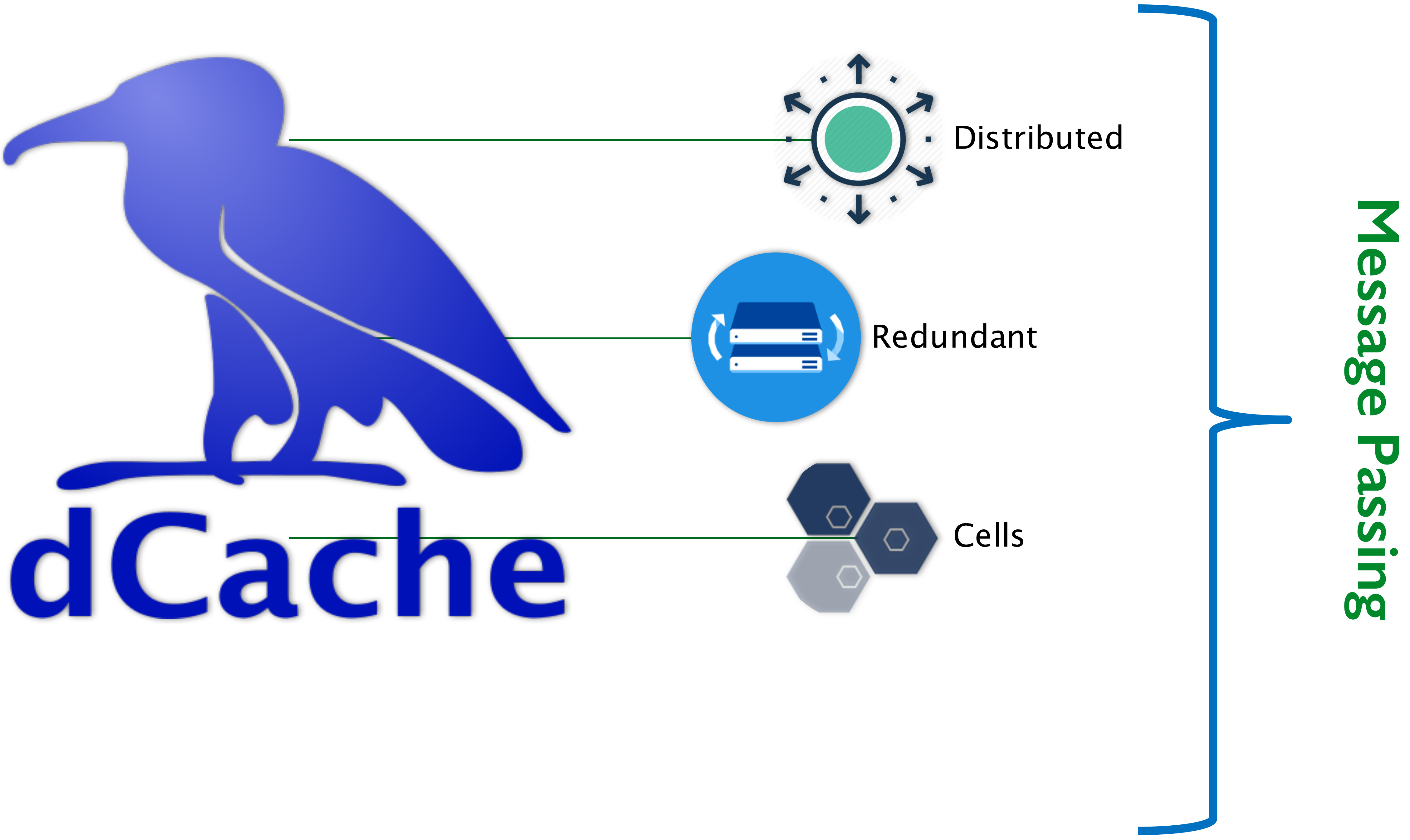
NDGF Nordic DataGrid Facility

INDIGO - DataCloud

DESY

HELMHOLTZ ASSOCIATION

LSDMA

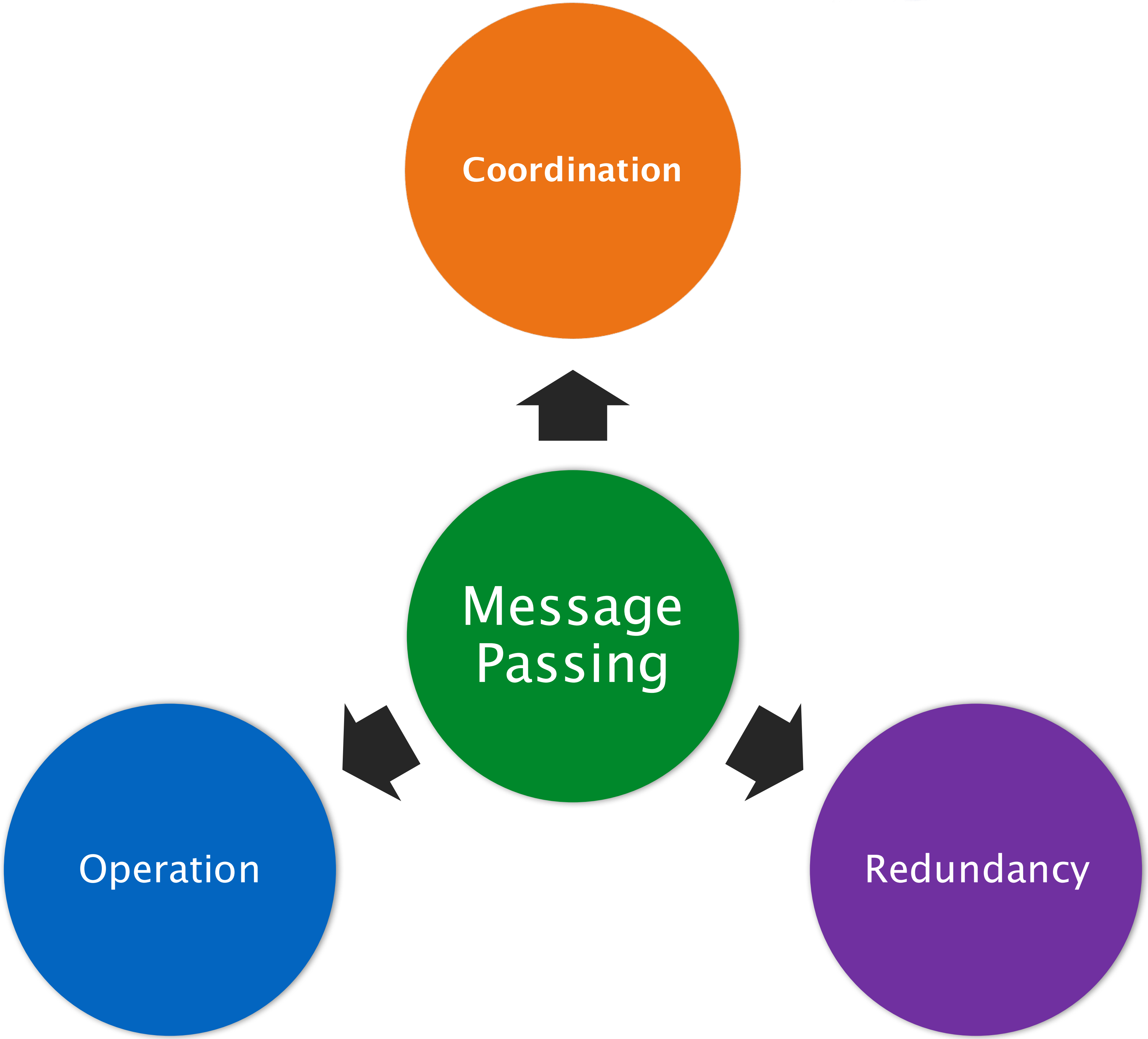


Distributed

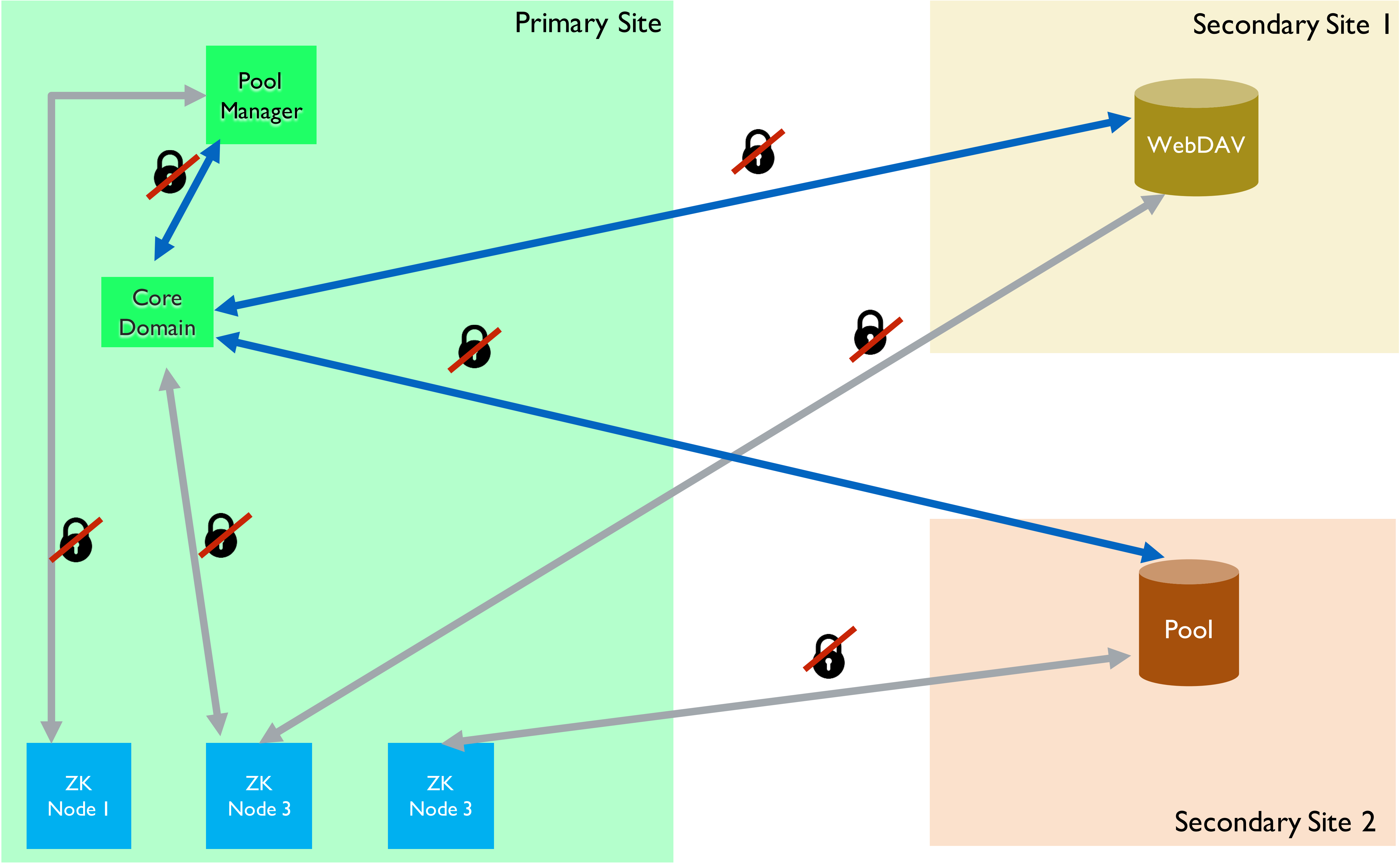
Redundant

Cells

Message Passing


Coordination
Message Passing
Operation
Redundancy

Multi-site deployment



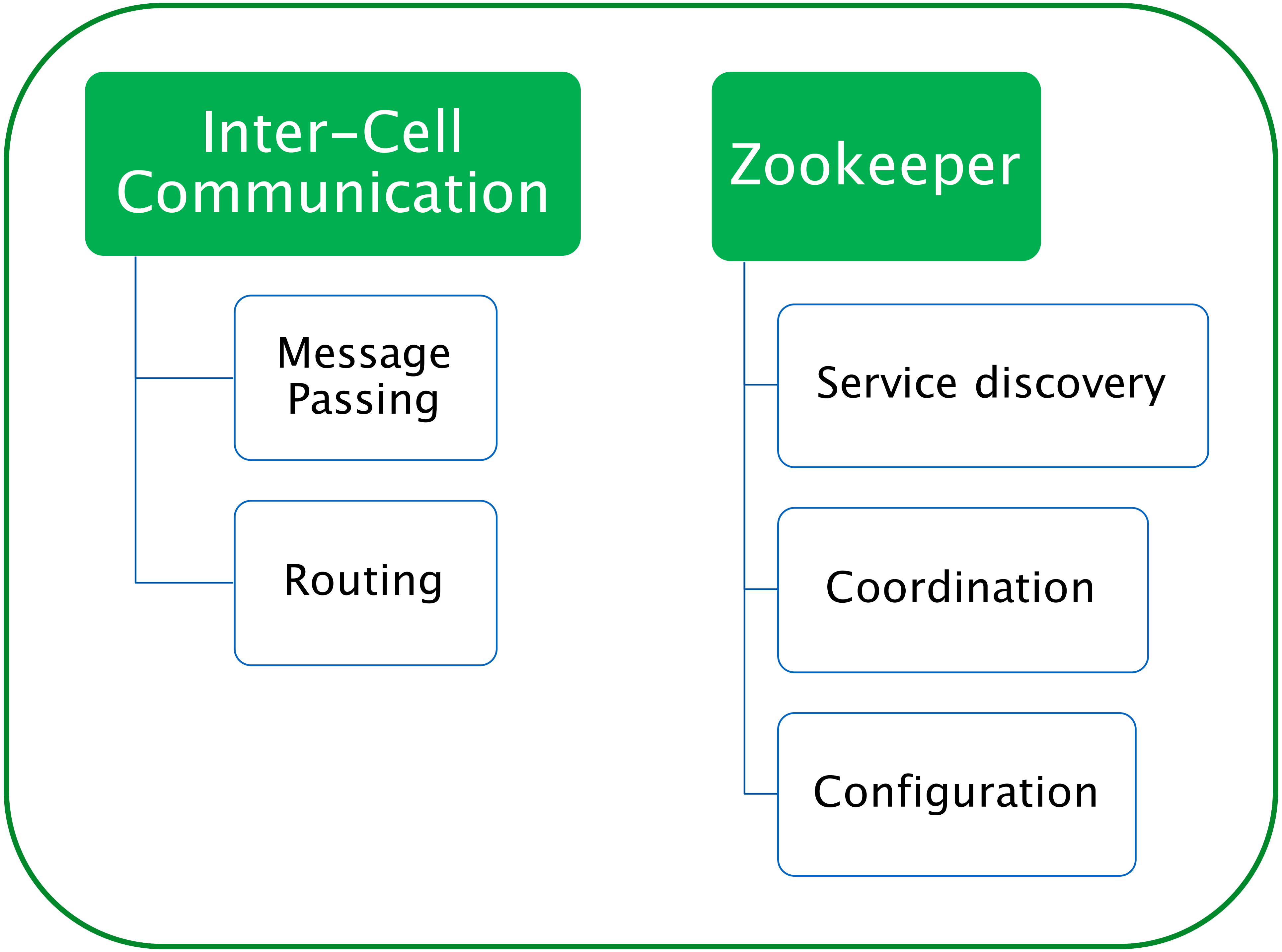
Motivation

- Federated dCache
  - Multi-site Deployment
  - Separated Geographically

- Secure over-the-Network communications

- Requirements based on Joint-Russian-German Project
  - NRC “Kurchatov Institute”, Moscow
  - JINR, Dubna
  - DESY Hamburg

Internal dCache Communications



Inter-Cell Communication

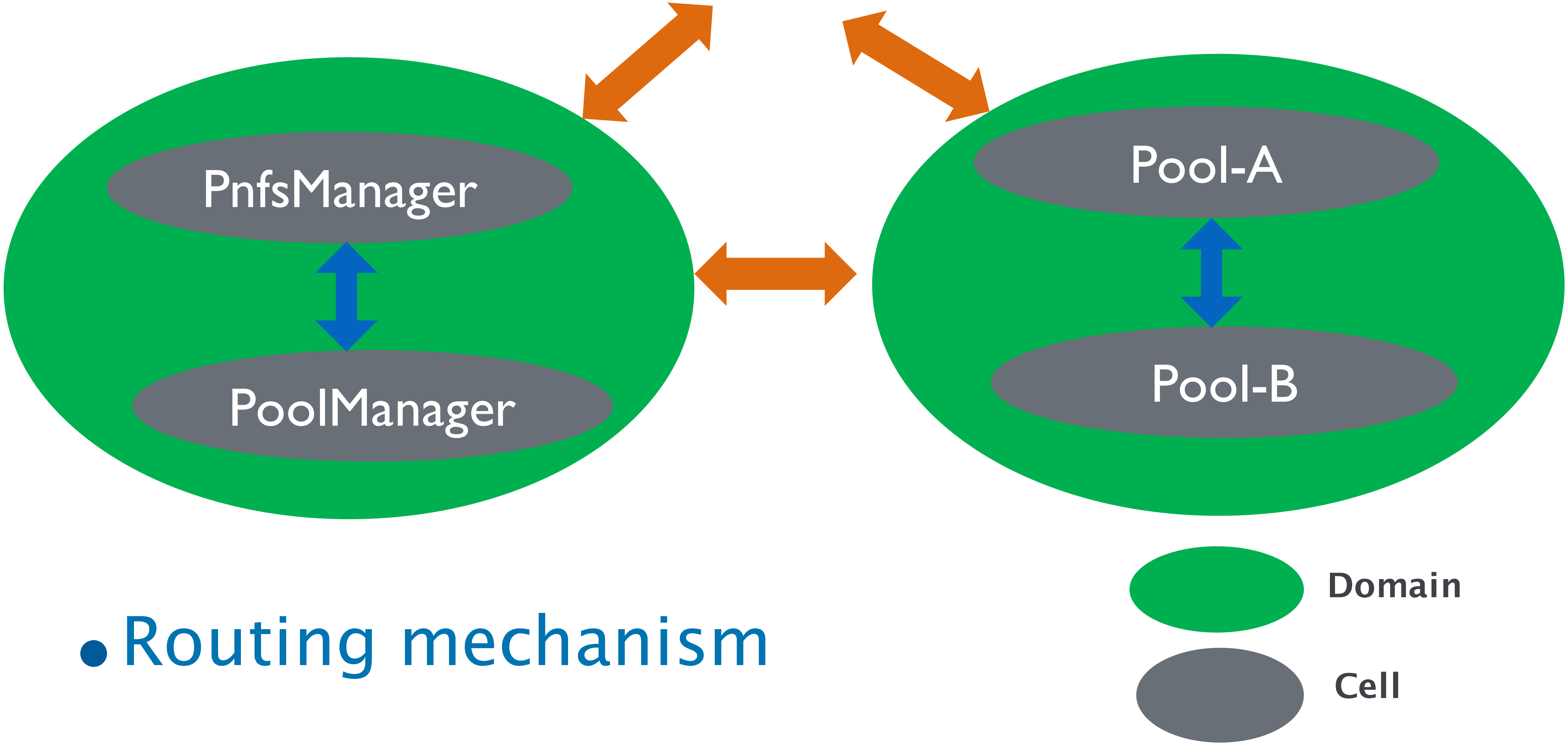
- Message Passing
- Routing

Zookeeper

- Service discovery
- Coordination
- Configuration

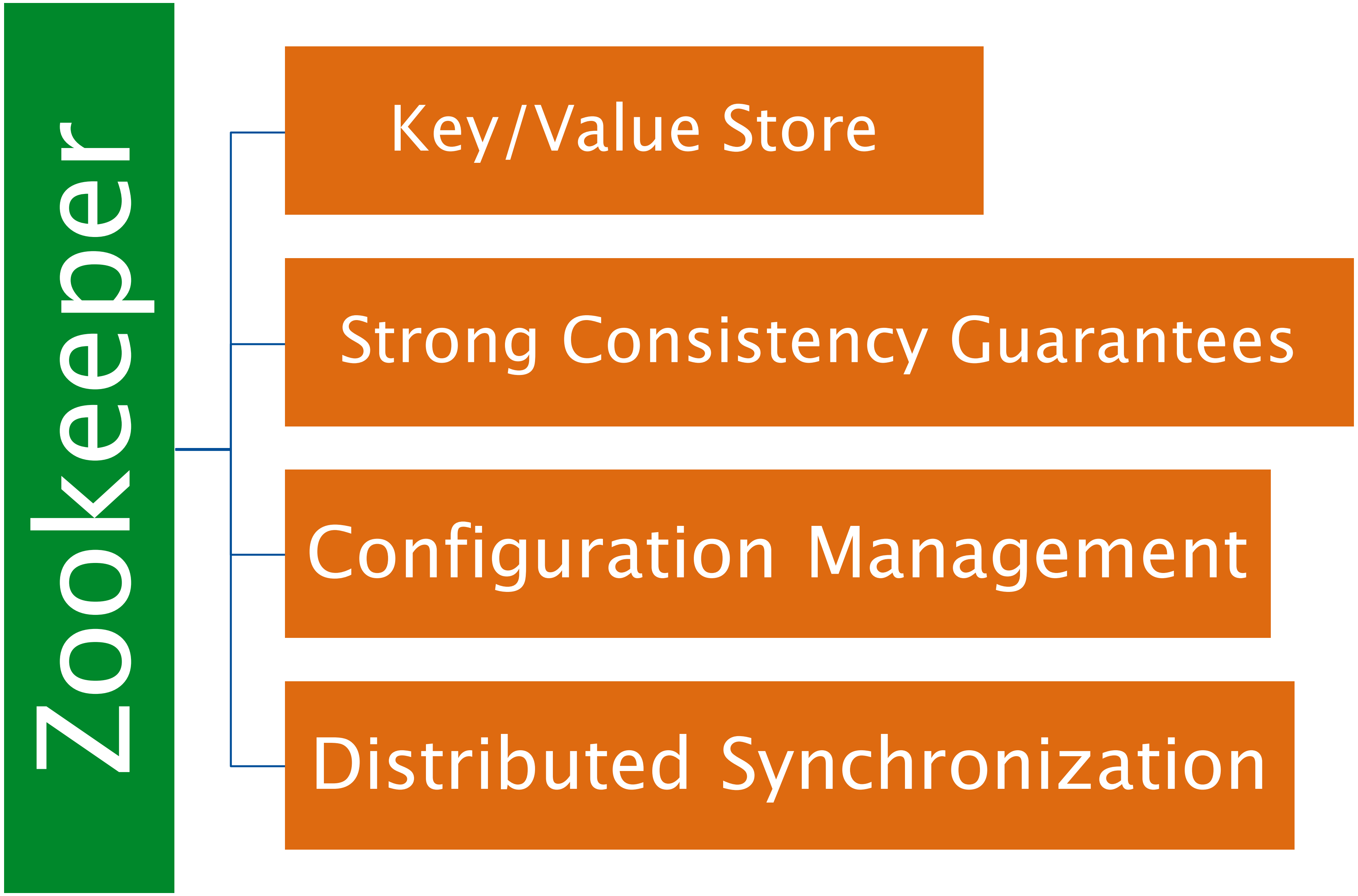
Cells

- Smallest addressable unit in dCache
- Cells have names



- Routing mechanism

Zookeeper



Zookeeper

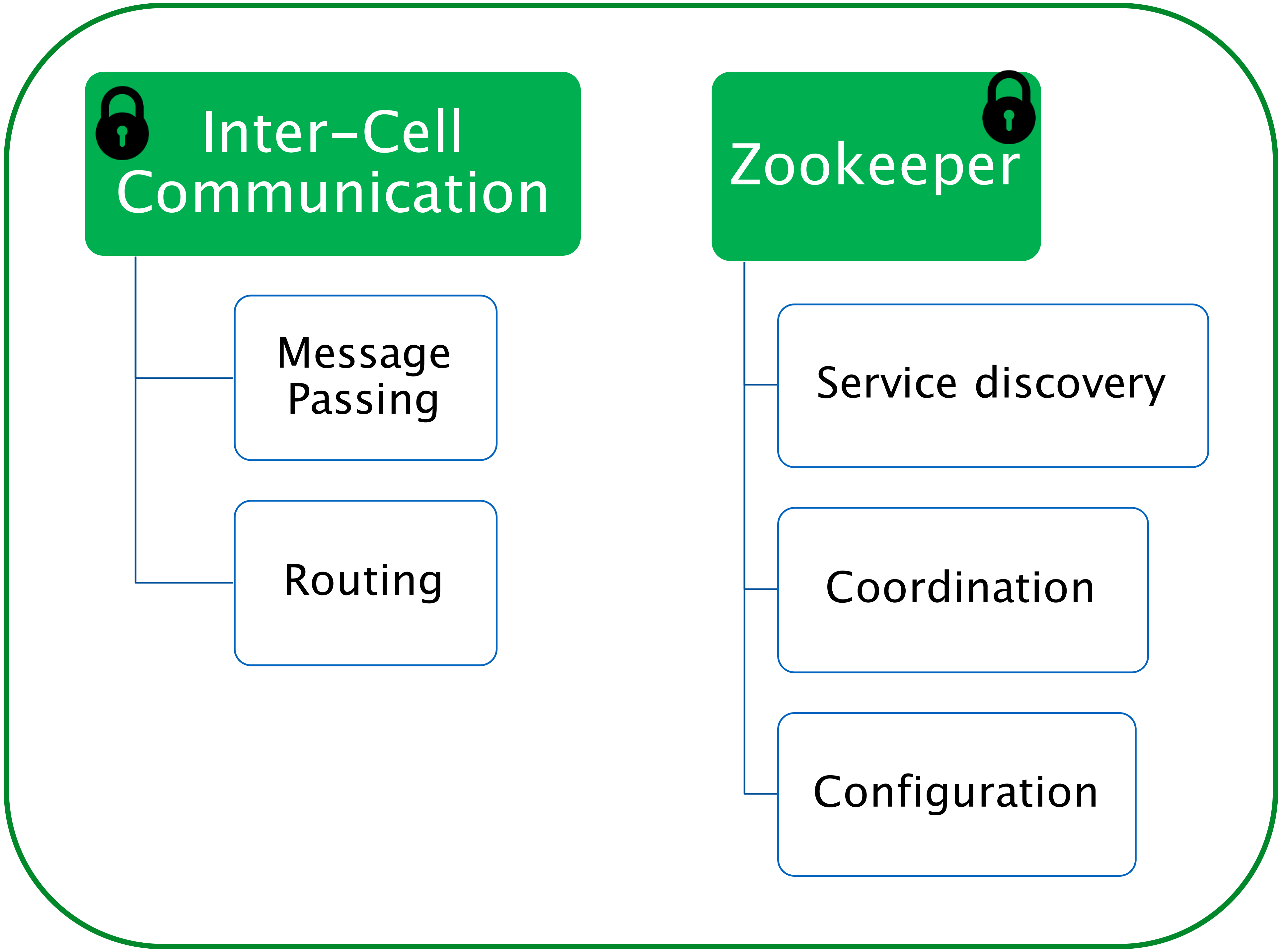
Key/Value Store

Strong Consistency Guarantees

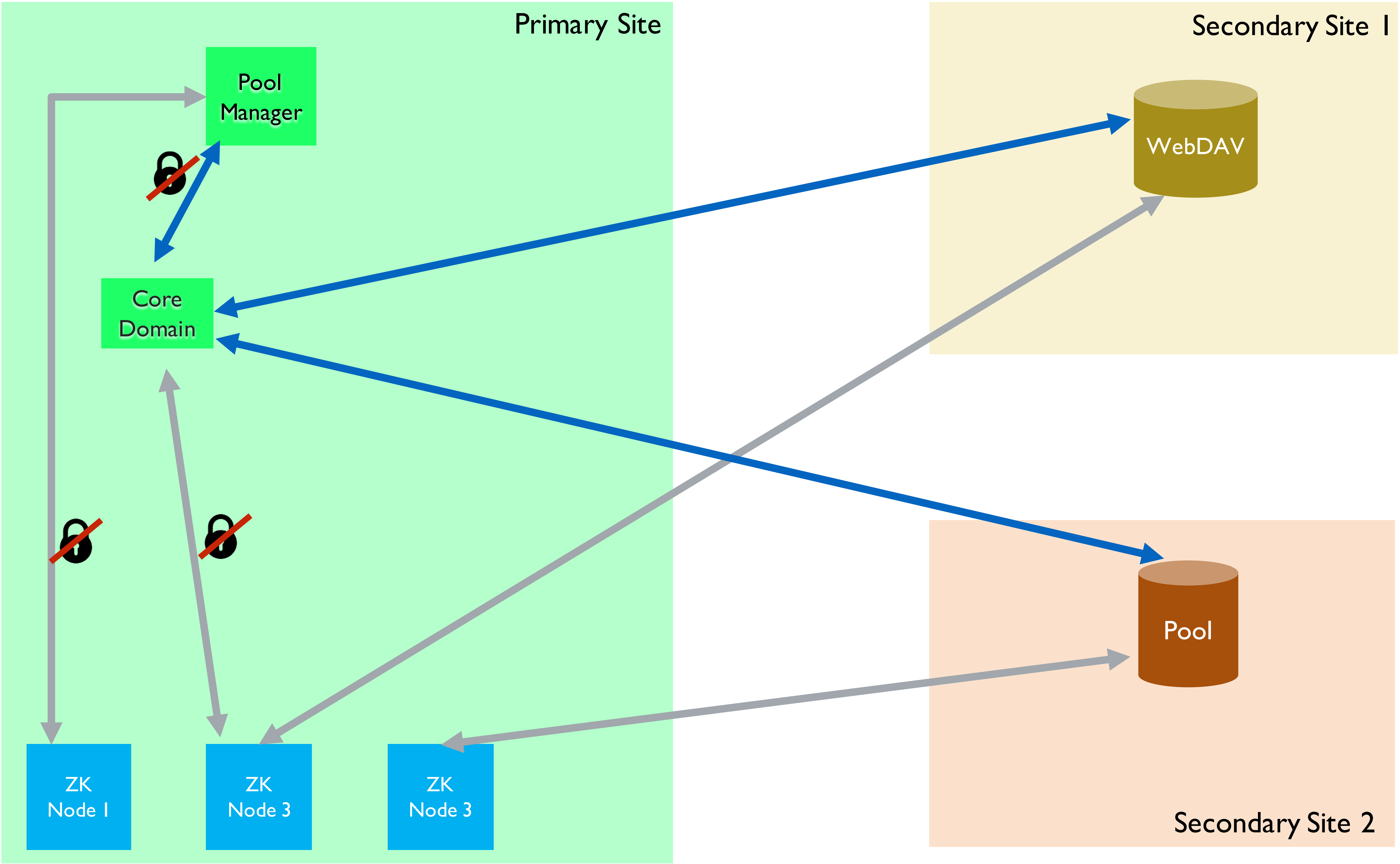
Configuration Management

Distributed Synchronization

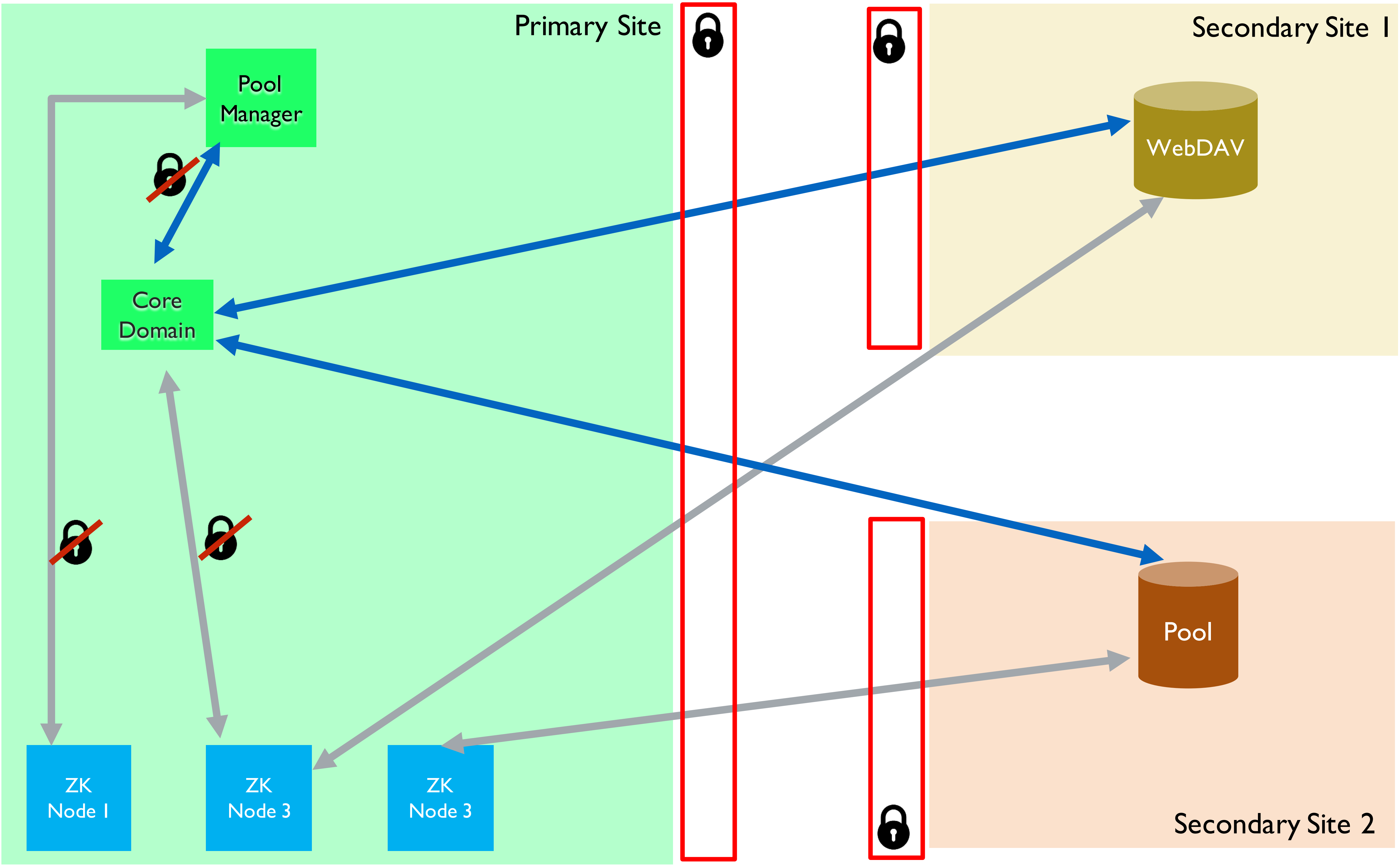
What we want to achieve ..



Multi-site deployment

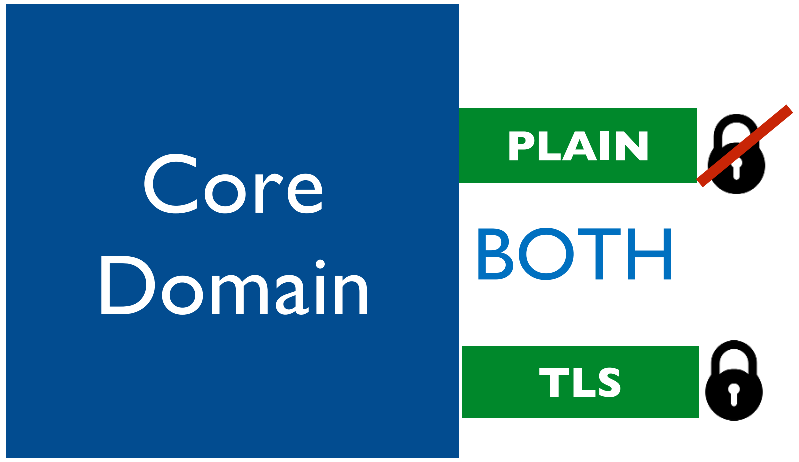


Multi-site deployment



Secure Cell Communications

dcache.broker.core.channel.security



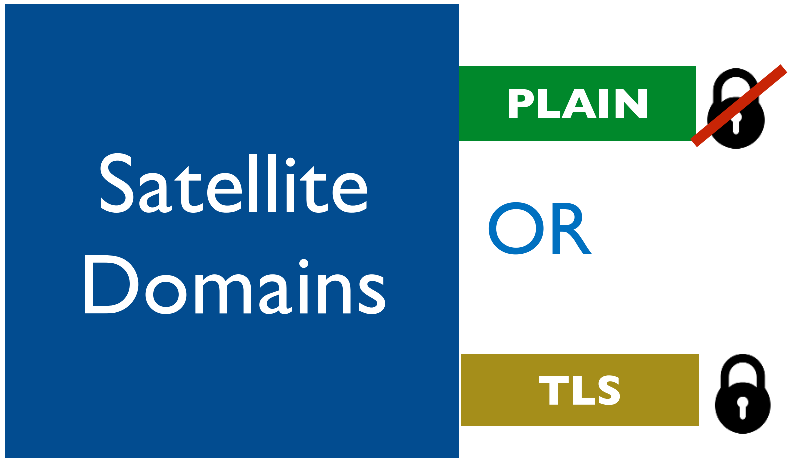
Core Domain

PLAIN

BOTH

TLS

- Support both TLS and Plain communication
- Disable encryption for all messages on the internal network



Satellite Domains

PLAIN

OR

TLS

dcache.broker.satellite.channel.security

Secure Communications

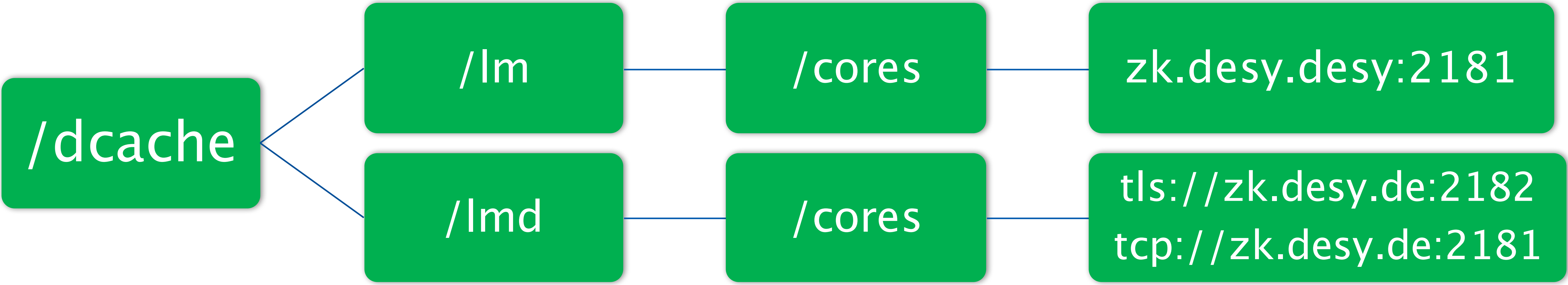
- dcache.broker.channel.credential.key
- dcache.broker.channel.credential.cert
- dcache.broker.channel.capath

Rely on TLS authentication

Zookeeper

- Stable release 3.4.x
- No support for TLS in the stable release
- Support for TLS comes in 3.5.x and 3.6.x

Zookeeper Backwards Compatible



Zookeeper with Stunnel

- Proxy designed to add TLS encryption functionality
  - without any changes in the programs' code.
- Provides
  - Security
  - Portability
  - Scalability (including load-balancing)

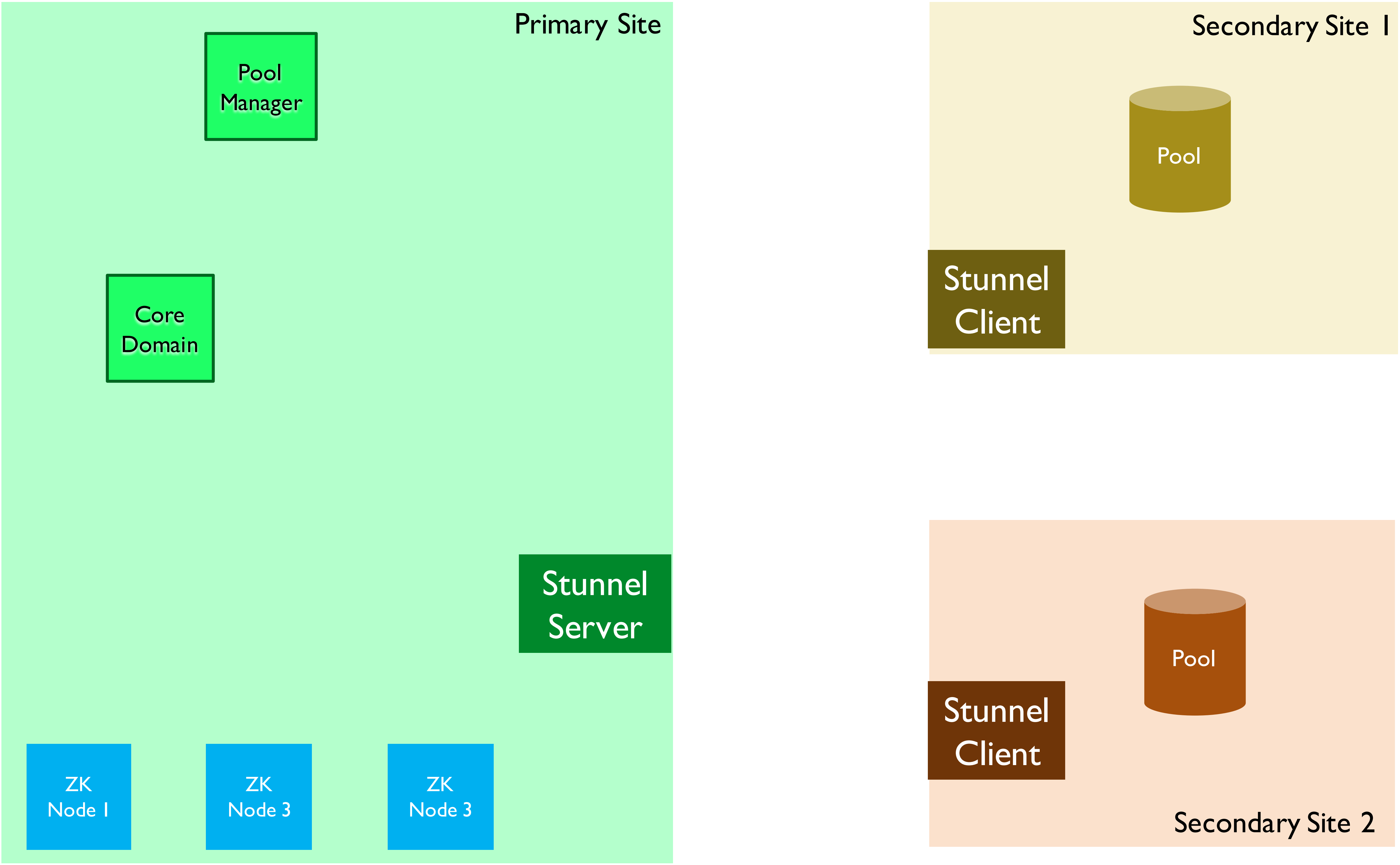
SERVER

```
[zookeeper]
accept = 2182
connect = zoocluster1.noname.de:2181
connect = zoocluster2.noname.de:2181
cert = /etc/stunnel/stunnel.pem
checkHost = zooclient1.noname.de
checkHost = zooclient2.noname.de
CAPath = /opt/noname/certs
```

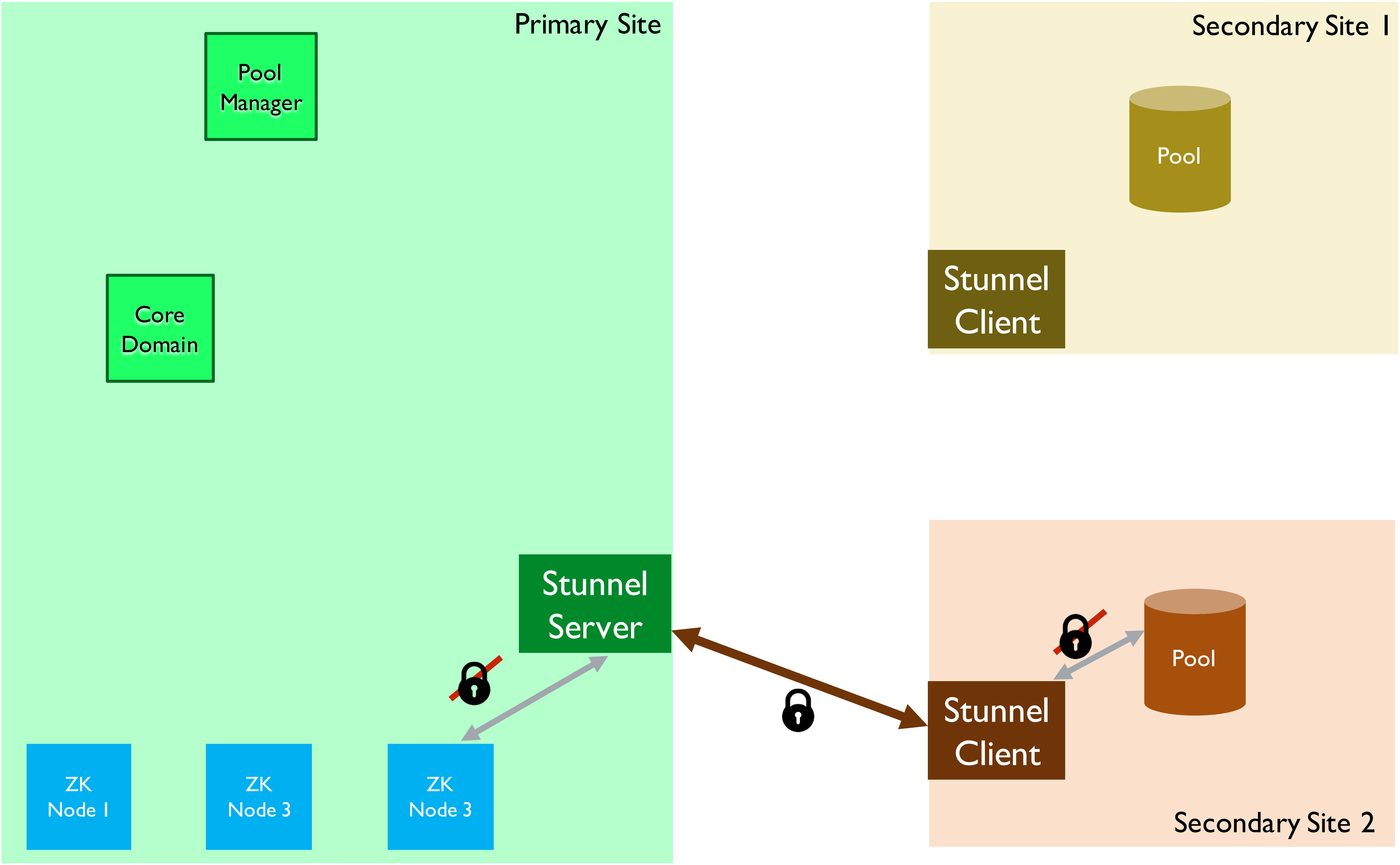
CLIENT

```
[zookeeper]
client = yes
accept = 2181
connect = stunnel.noname.de:2182
;verify = 2
cert = /etc/stunnel/stunnel.pem
CApath = /opt/noname/certs
checkHost = stunnel.noname.de
;OCSPaia = yes
```

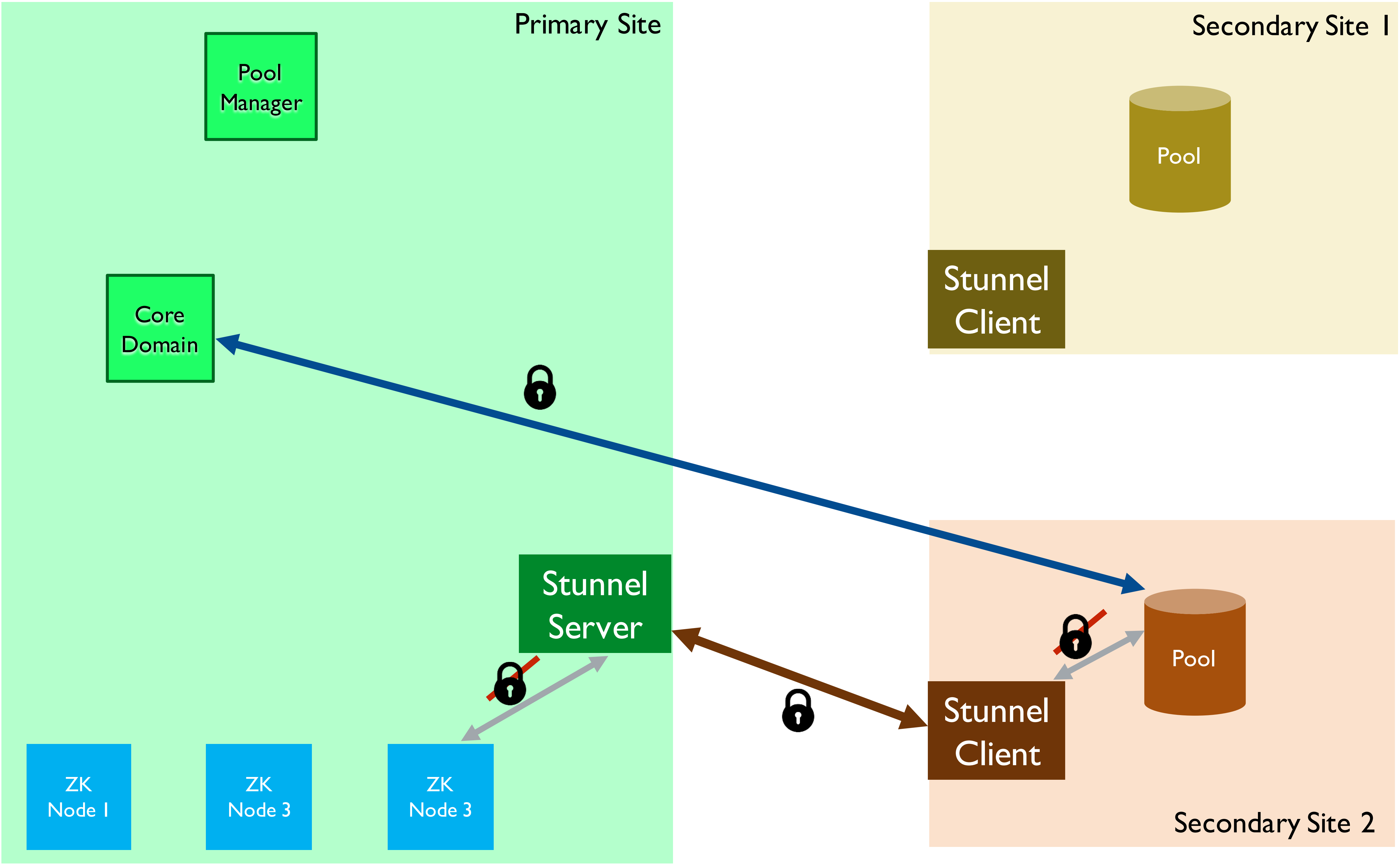
Zookeeper with Stunnel



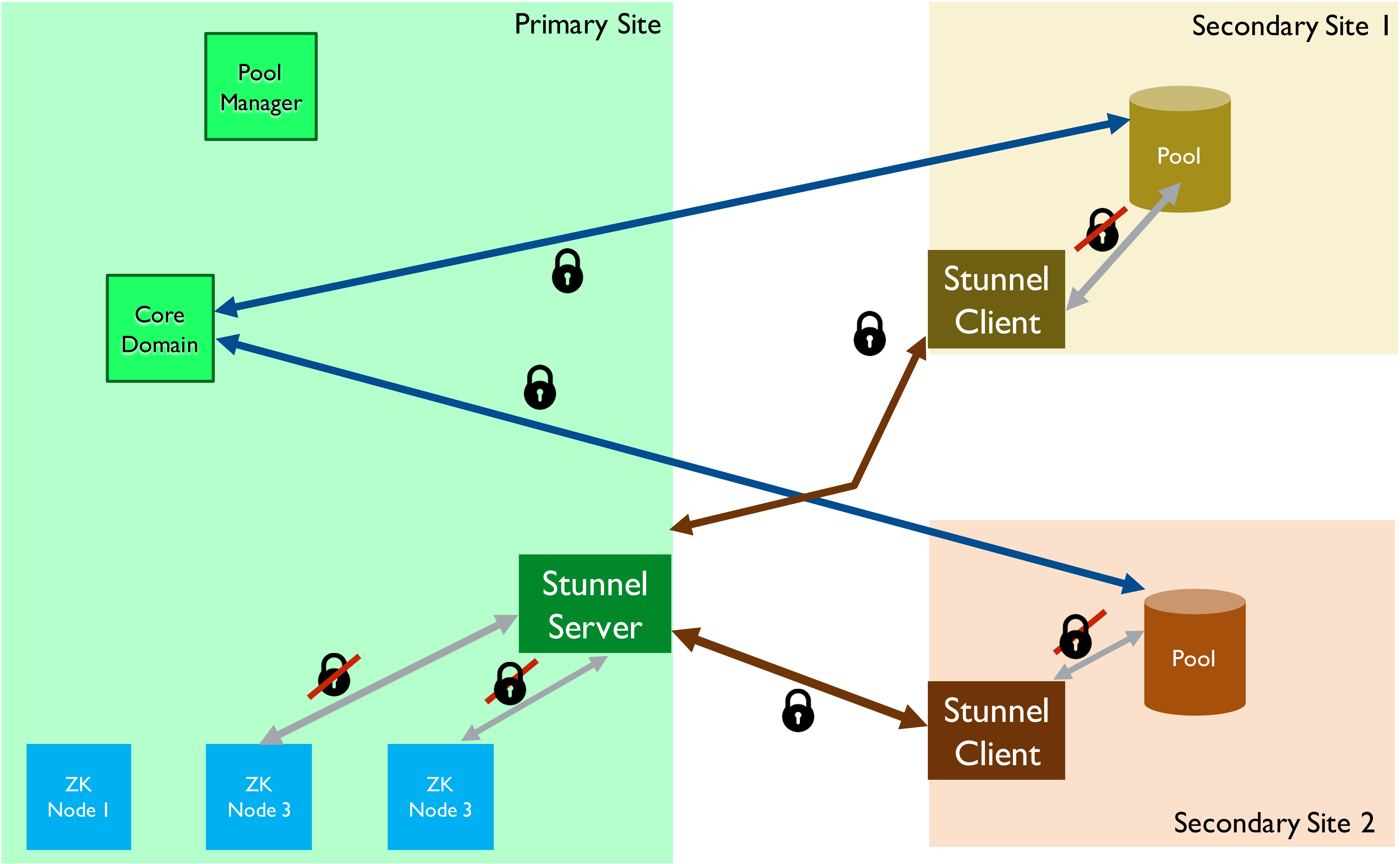
Zookeeper with Stunnel



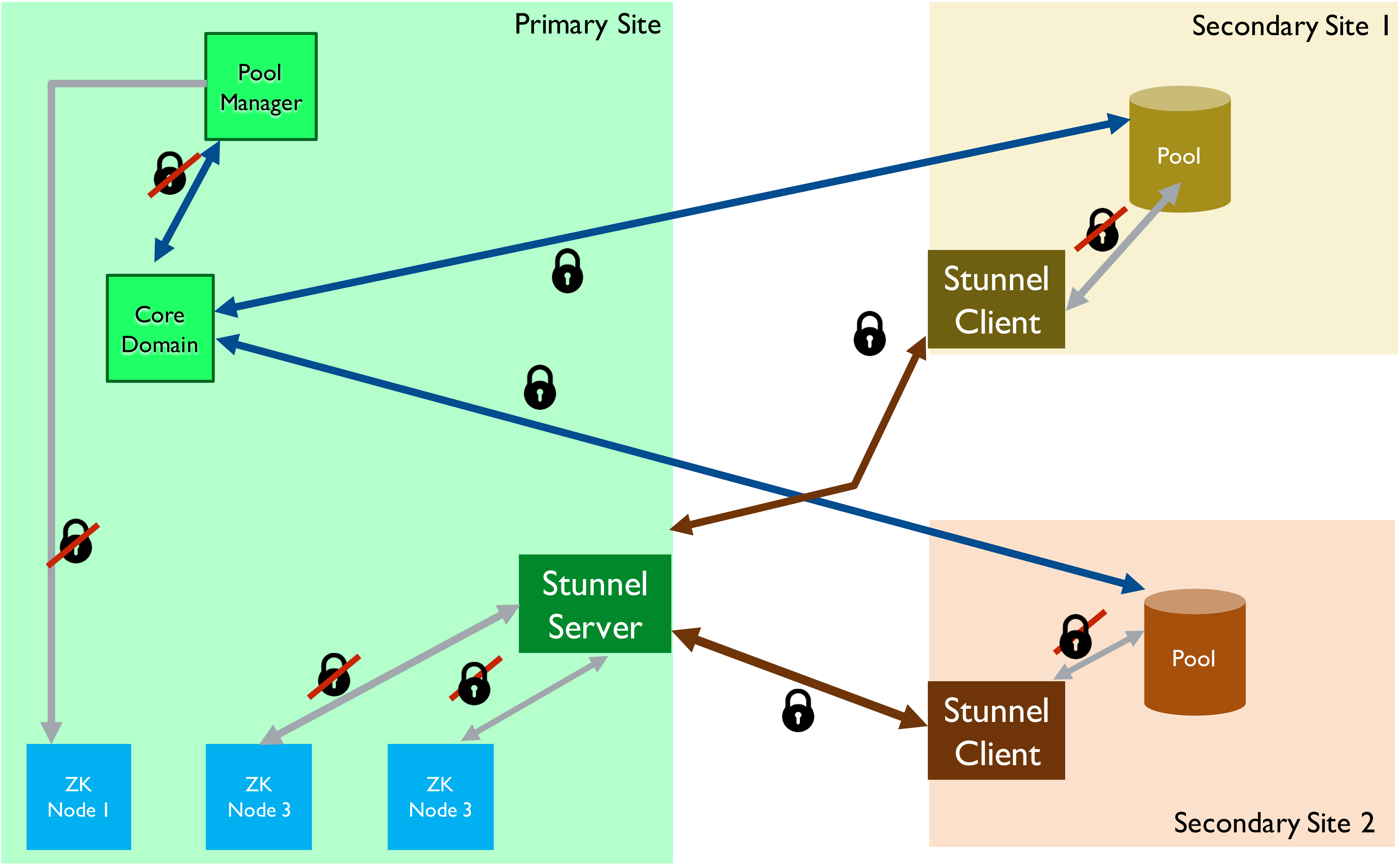
Zookeeper with Stunnel



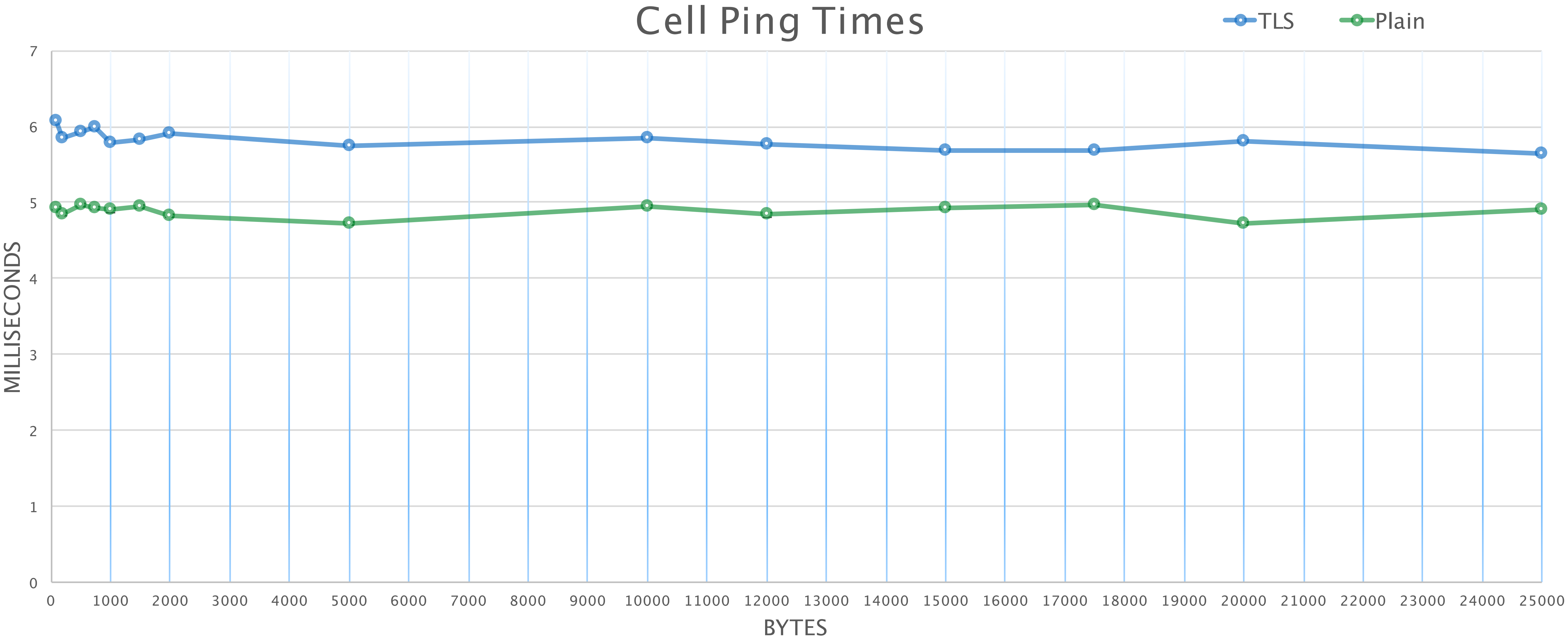
Zookeeper with Stunnel



Zookeeper with Stunnel



Overhead


Cell Ping Times
TLS
Plain
MILLISECONDS
0
1
2
3
4
5
6
7
BYTES
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000
11000
12000
13000
14000
15000
16000
17000
18000
19000
20000
21000
22000
23000
24000
25000

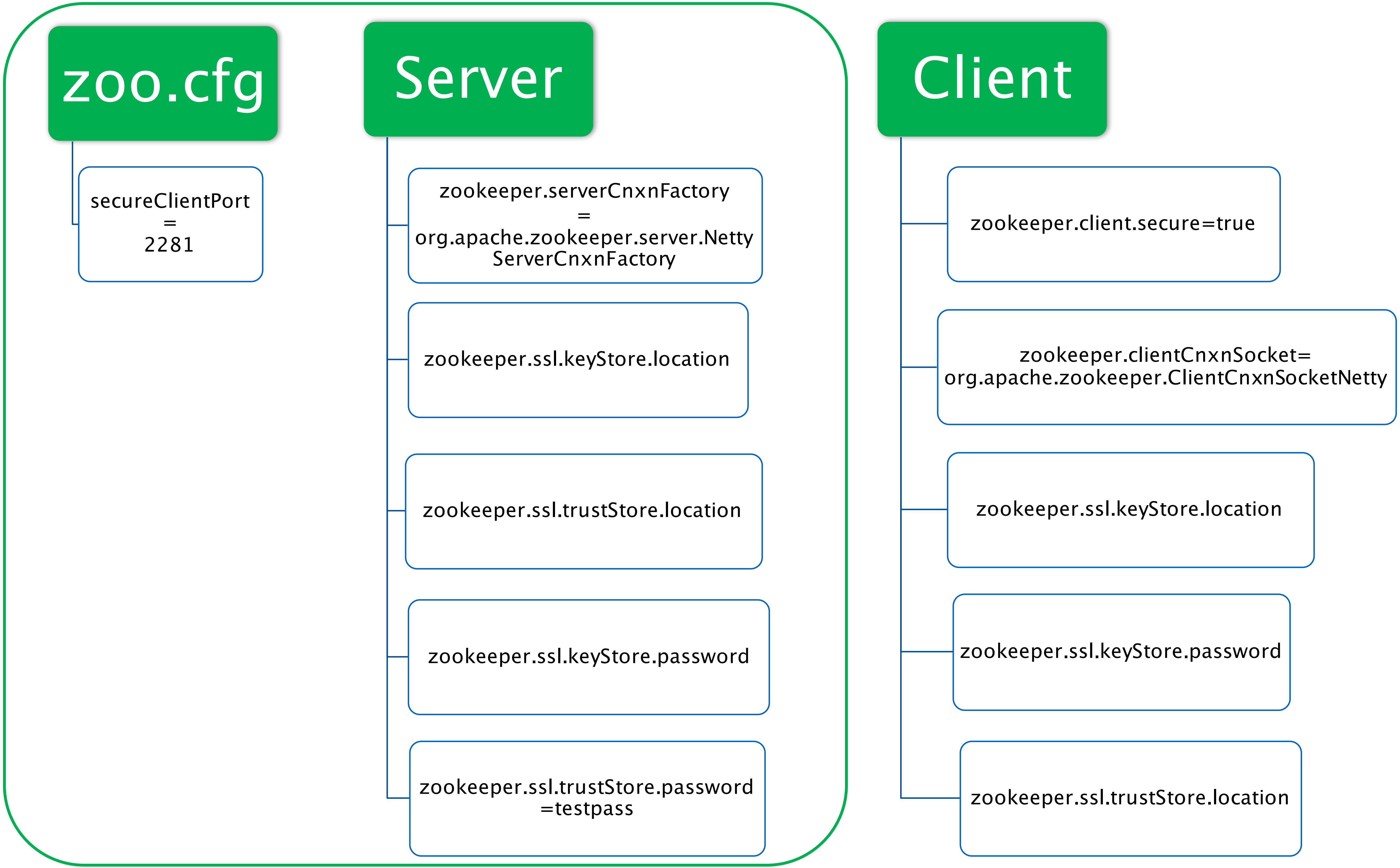
Recap

- dCache multi-site deployment
- Secure Cell-Communication
  - With TLS Authentication
- Secure Zookeeper
  - 3.5.x and 3.6.x
- Stunnel for Zookeeper 3.4.x

Thank You !!

Bytes	TLS	Stddev (TLS)	Plain	Stddev (Plain
100	6.066532	0.962029	4.923287	1.528073
200	5.852289	1.207879	4.845971	1.083889
500	5.92067	1.150411	4.965656	1.073847
750	5.991981	0.971823	4.92993	1.25704
1000	5.792476	0.965675	4.899043	1.085029
1500	5.818405	1.268044	4.947244	1.215096
2000	5.910056	0.985793	4.833325	1.179955
5000	5.744266	1.034607	4.716026	1.116742
10000	5.842495	1.147705	4.949989	1.120223
12000	5.771063	1.011539	4.836352	1.182209
15000	5.681811	0.996409	4.930635	1.088731
17500	5.687488	1.056684	4.970123	1.083949
20000	5.802021	1.007485	4.717774	1.14542
25000	5.640754	0.901774	4.913348	1.39213

Zookeeper 3.5.x and 3.6.x



zoo.cfg

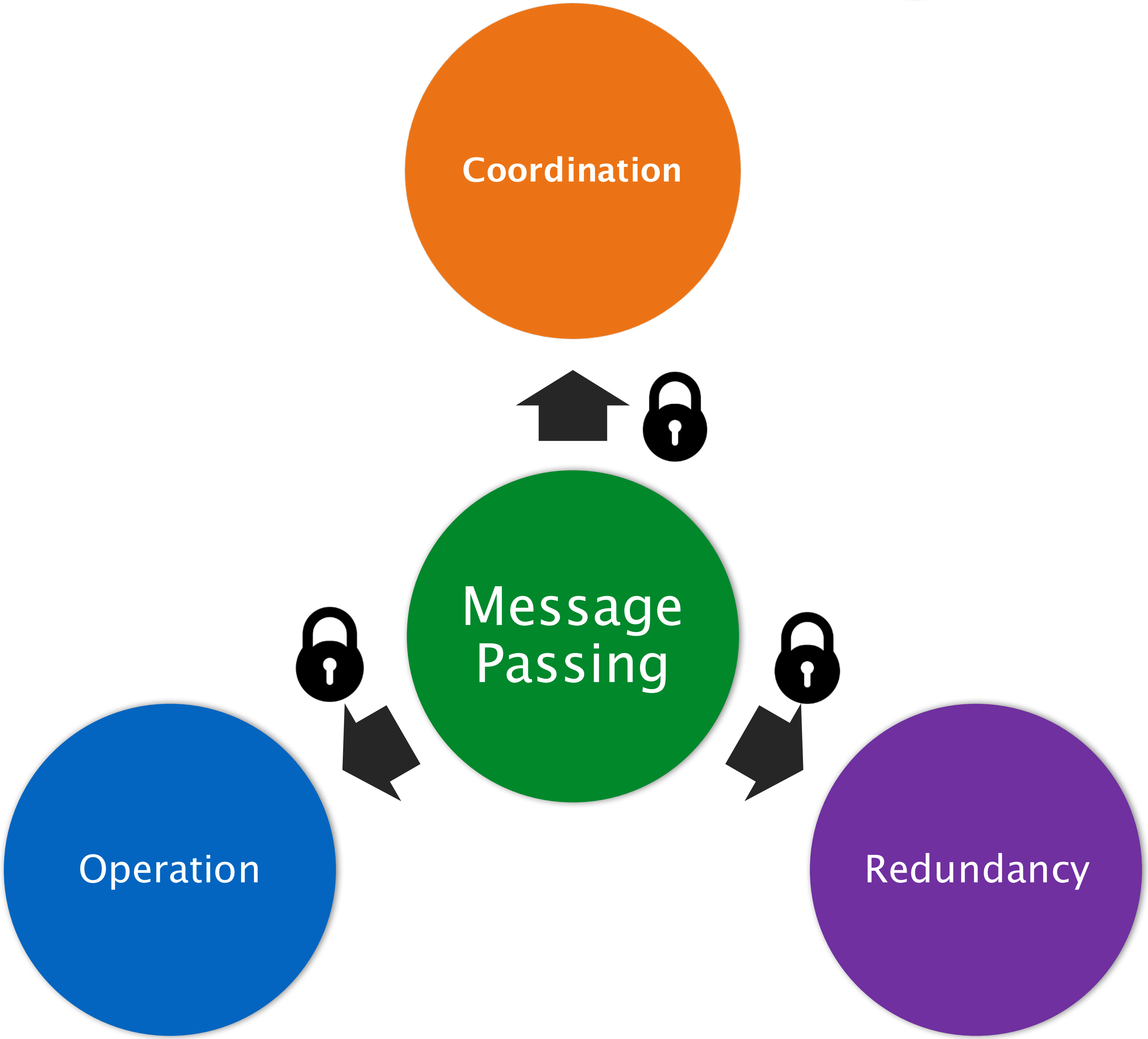
- secureClientPort = 2281

Server

- zookeeper.serverCnxnFactory = org.apache.zookeeper.server.NettyServerCnxnFactory
- zookeeper.ssl.keyStore.location
- zookeeper.ssl.trustStore.location
- zookeeper.ssl.keyStore.password
- zookeeper.ssl.trustStore.password =testpass

Client

- zookeeper.client.secure=true
- zookeeper.clientCnxnSocket= org.apache.zookeeper.ClientCnxnSocketNetty
- zookeeper.ssl.keyStore.location
- zookeeper.ssl.keyStore.password
- zookeeper.ssl.trustStore.location


Coordination
Message Passing
Operation
Redundancy