Microsoft

Application Hardening mit Dapr

Ricardo Niepel

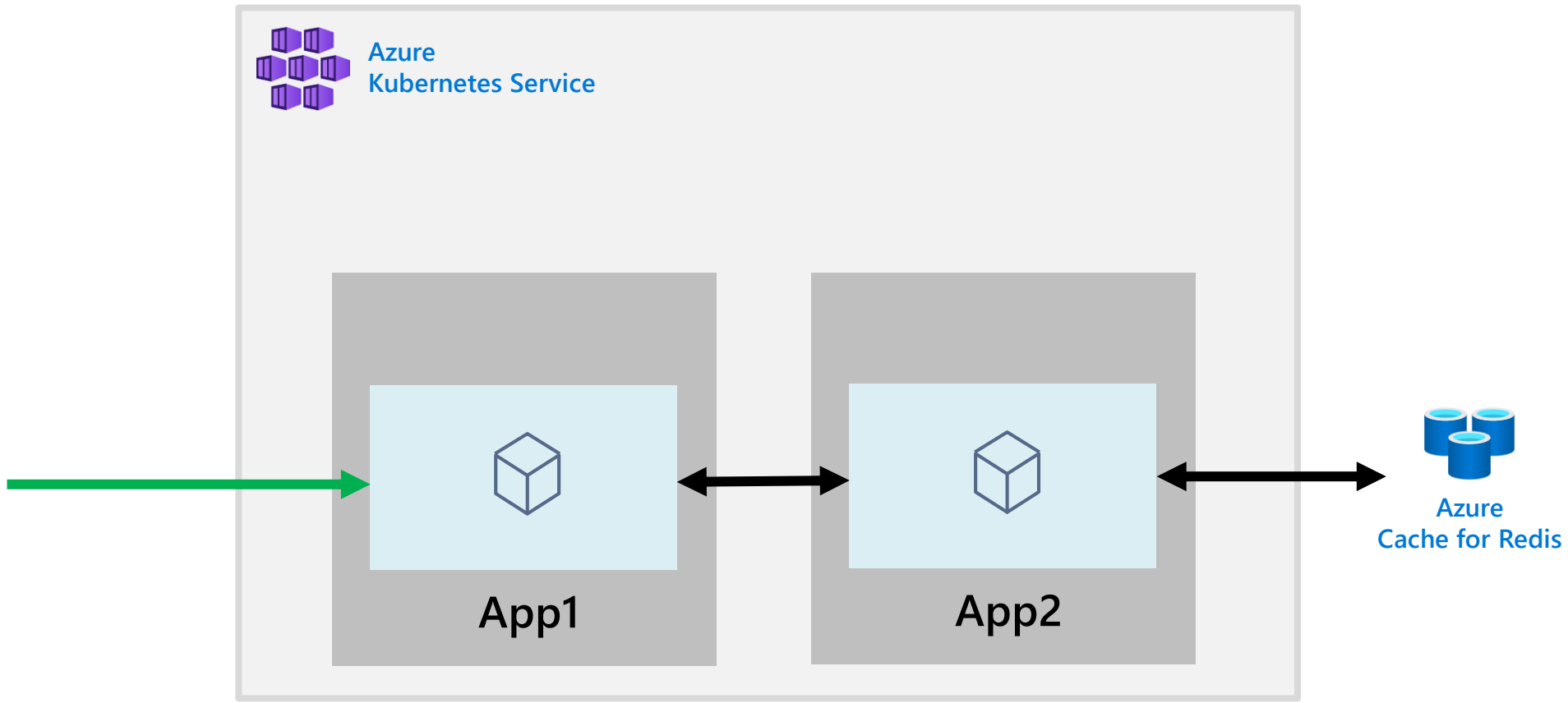
#SummITup

Agenda

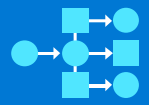
- Bestehende Applikation “Daprizen”
- mTLS und SPIFFE Identitäten hinzufügen
- Aufrufbare HTTP Operationen einschränken
- Zugriffsschlüssel sicher speichern
- Die Nutzung einschränken von
  - Datenspeicher
  - Nachrichtenbroker
  - Schlüsselspeicher

Legend

explicitly allowed dataflow



Dapr Bausteine



Service-to-service invocation

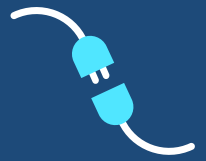
Durchführen von direkten und sicheren Service-to-Service-Methodenaufrufen

State management

Erstellen von lang laufenden, zustands-behafteten Services

Publish and subscribe

Sicherer und skalierbarer Nachrichten-Austausch zwischen Services



Bindings (input/output)

Ereignisgetriebene Ausführung von Code durch zahlreiche Trigger

Eingabe- und Ausgabebindungen an externe Ressourcen, einschließlich Datenbanken und Warteschlangen

Actors

Kapseln von Code und Daten in wiederverwendbaren Aktoren als häufiges Microservices Entwurfsmuster

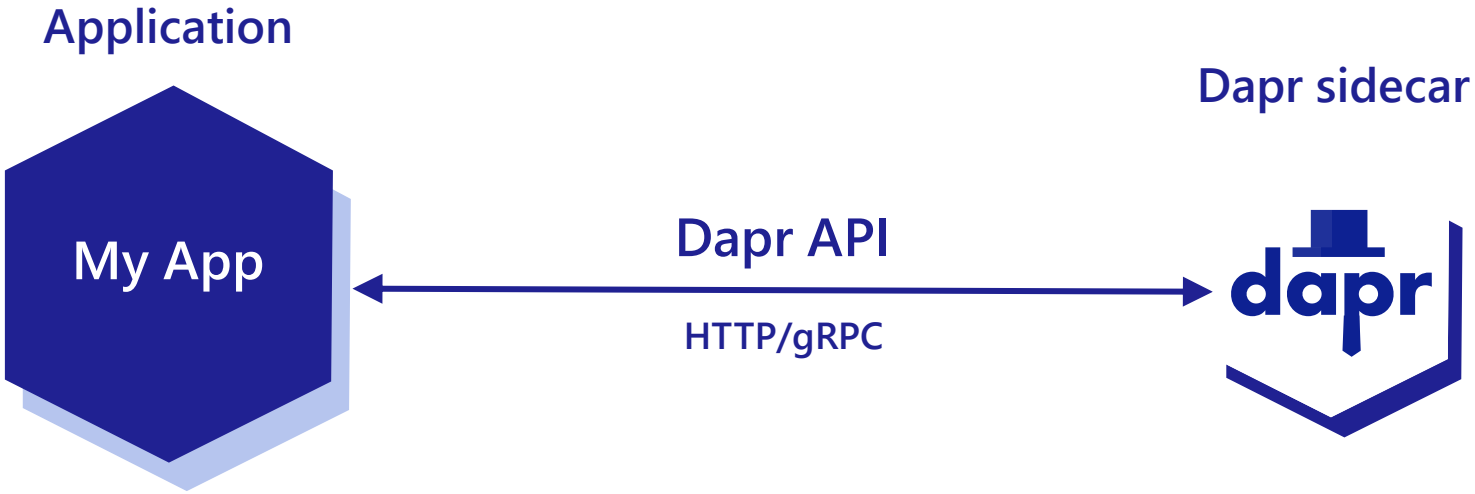
Observability

Überwachung und Messung aller Nachrichtenaufrufe zwischen Dapr-Systemdiensten, Komponenten und Anwendungen

Secrets

Sicherer Zugriff auf Schlüssel aus der Anwendung heraus

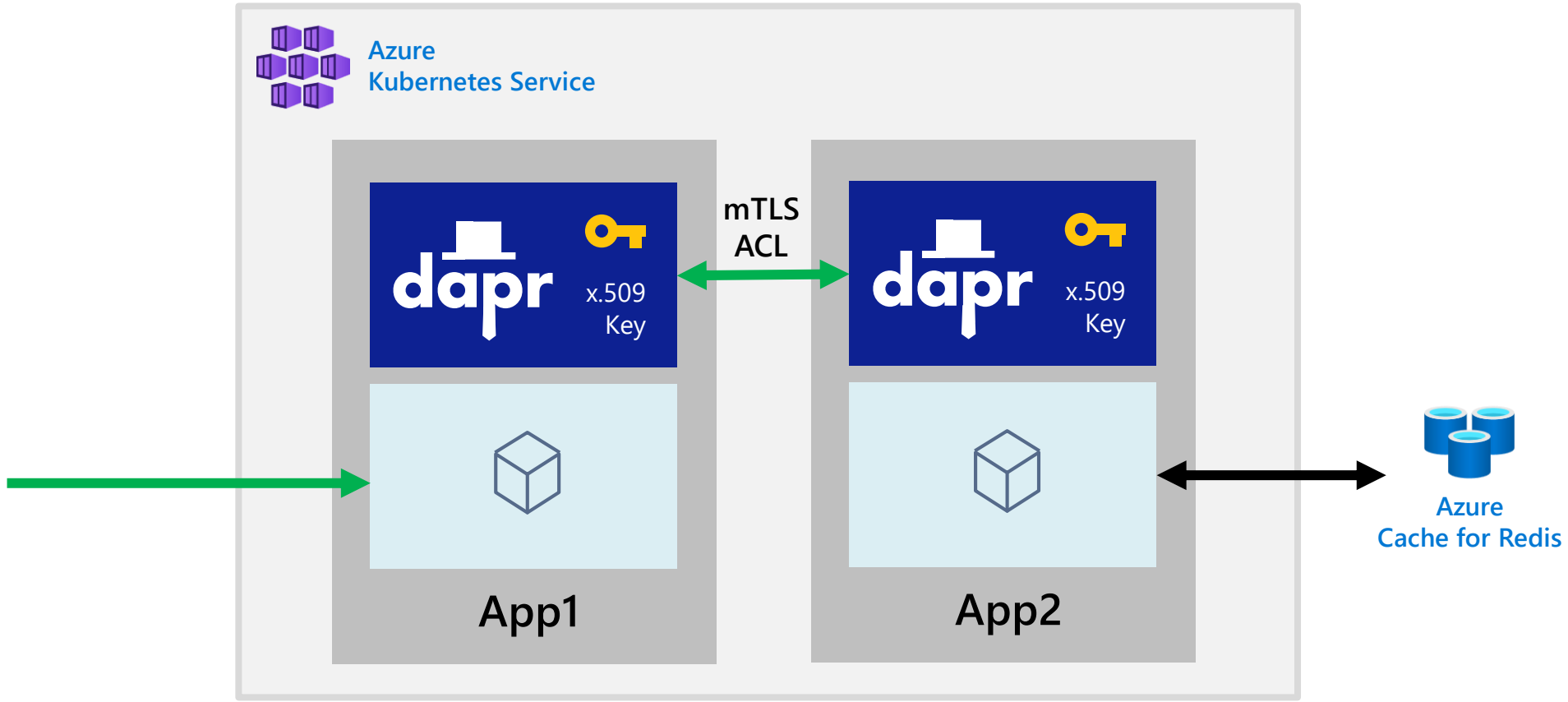
Dapr Sidecar Model




```
POST http://localhost:3500/v1.0/invoke/cart/method/neworder

GET http://localhost:3500/v1.0/state/inventory/item67

POST http://localhost:3500/v1.0/publish/shipping/orders

GET http://localhost:3500/v1.0/secrets/keyvault/password
```

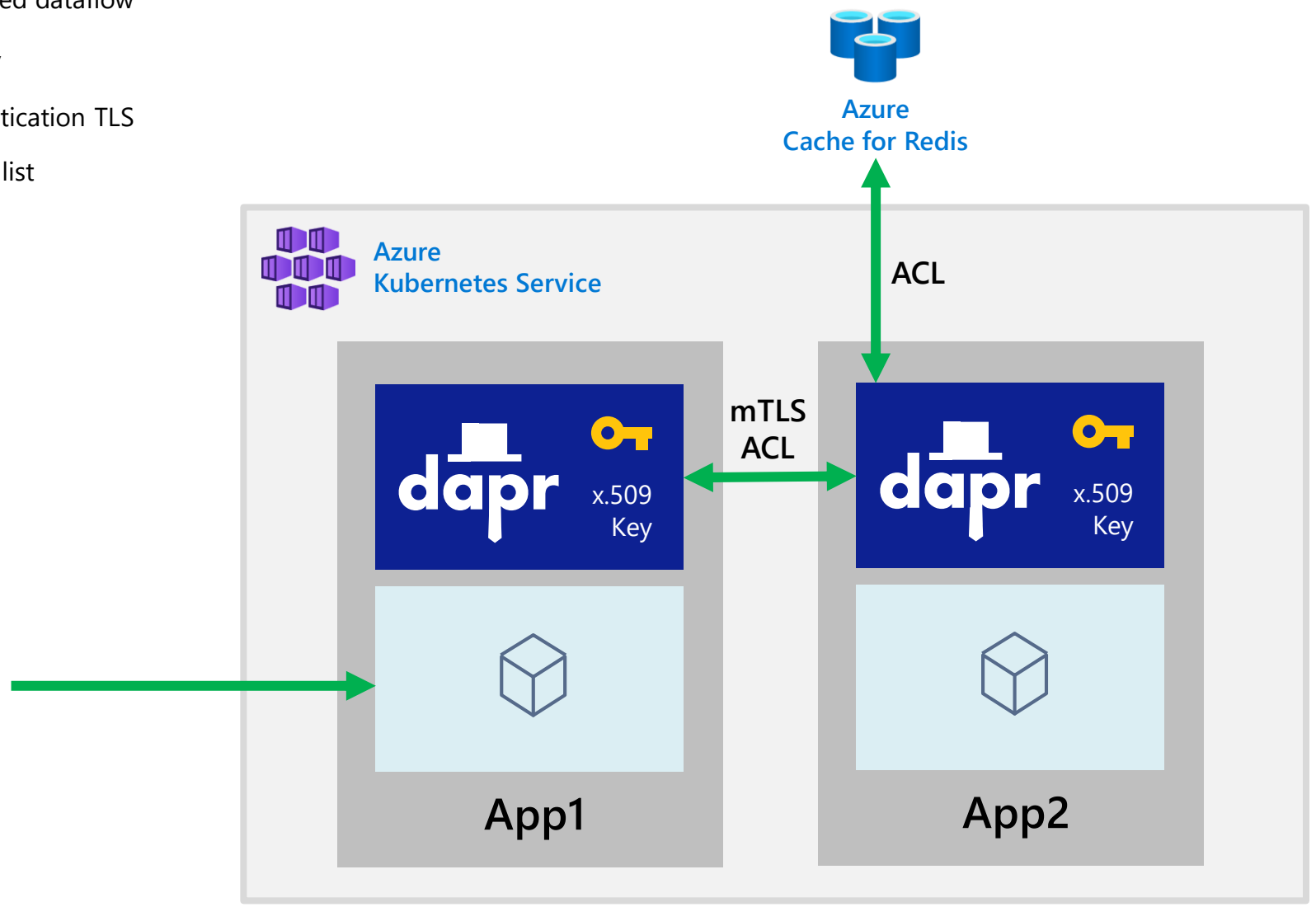
Legend

- explicitly allowed dataflow
- SPIFFE identity
- **mTLS** mutual authentication TLS
- **ACL** access control list



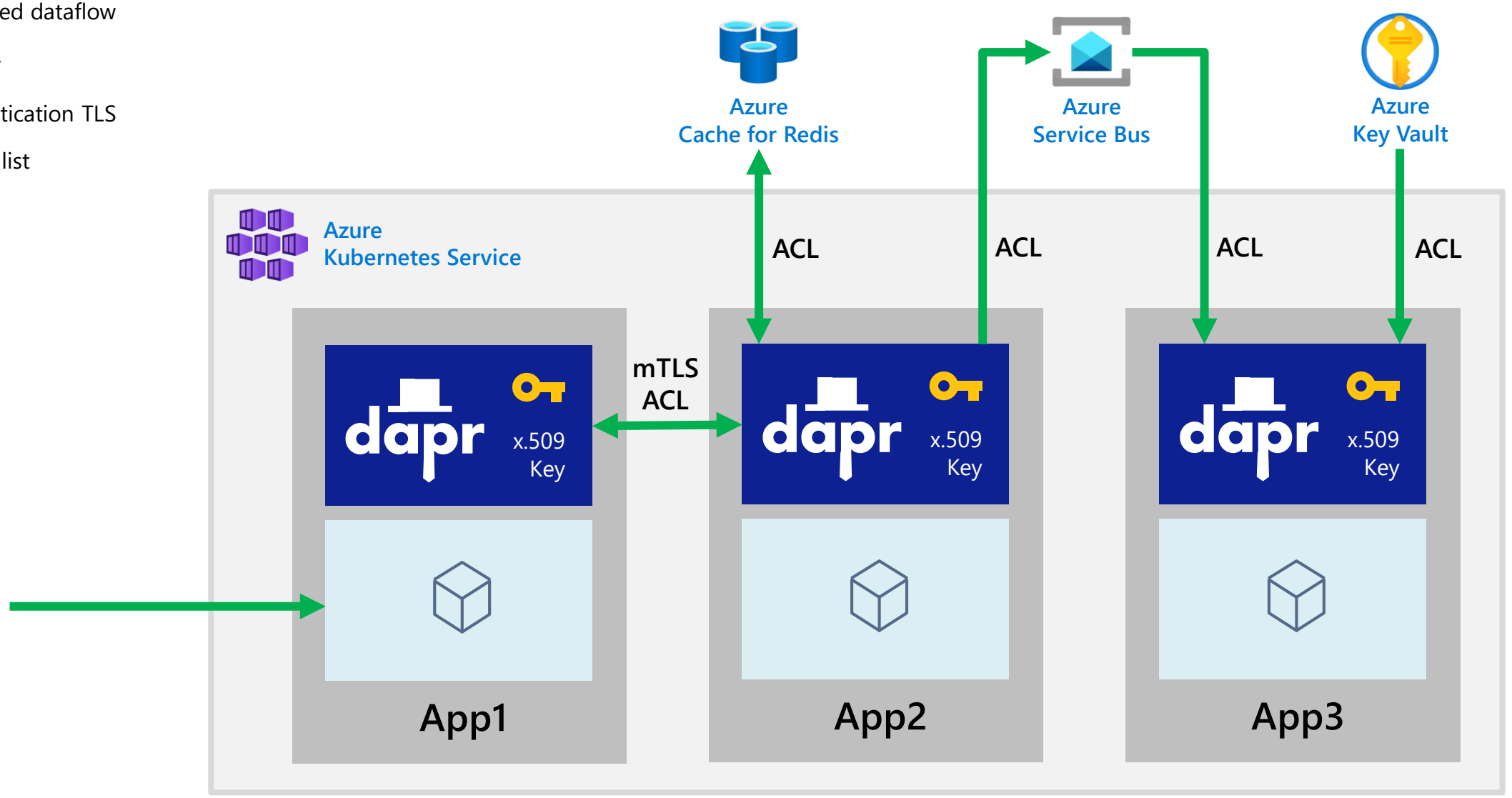
Legend

- explicitly allowed dataflow
- SPIFFE identity
- **mTLS** mutual authentication TLS
- **ACL** access control list

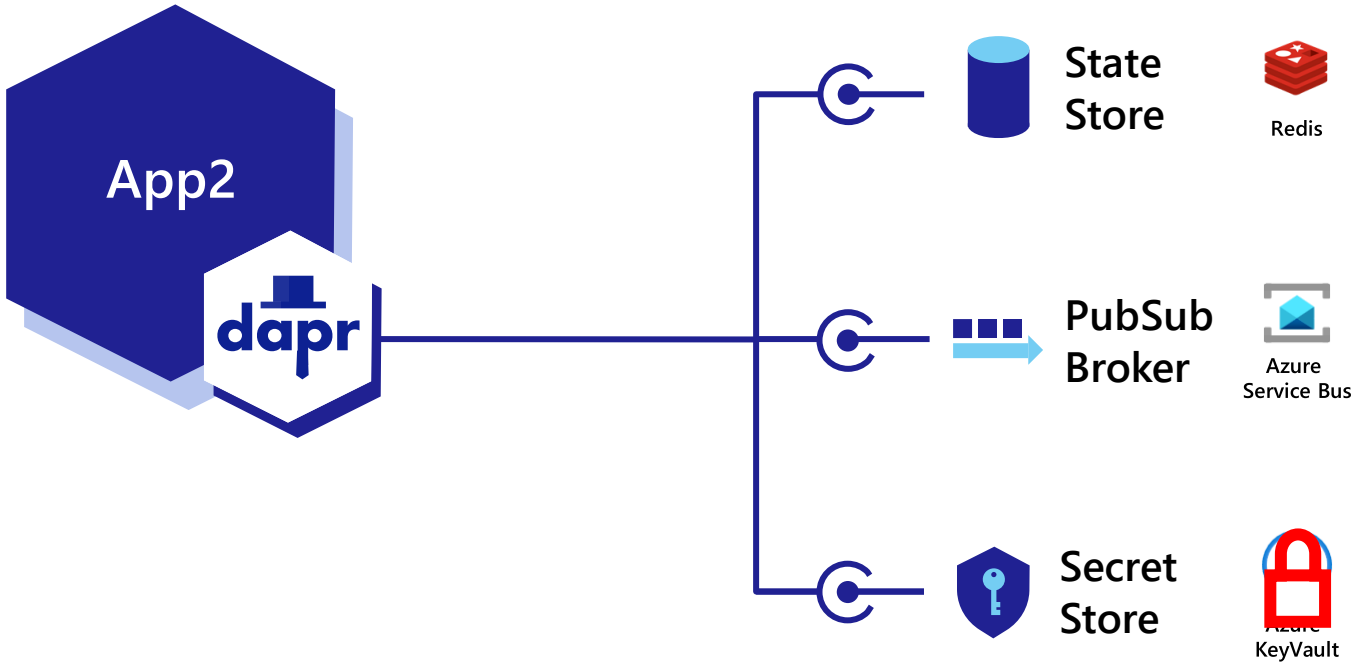


Legend

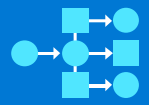
- explicitly allowed dataflow
- SPIFFE identity
- **mTLS** mutual authentication TLS
- **ACL** access control list



Dapr Komponenten Scopes



Dapr Bausteine



Service-to-service invocation

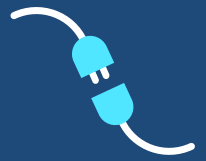
Durchführen von direkten und sicheren Service-to-Service-Methodenaufrufen

State management

Erstellen von lang laufenden, zustands-behafteten Services

Publish and subscribe

Sicherer und skalierbarer Nachrichten-Austausch zwischen Services



Bindings (input/output)

Ereignisgetriebene Ausführung von Code durch zahlreiche Trigger

Eingabe- und Ausgabebindungen an externe Ressourcen, einschließlich Datenbanken und Warteschlangen

Actors

Kapseln von Code und Daten in wiederverwendbaren Aktoren als häufiges Microservices Entwurfsmuster

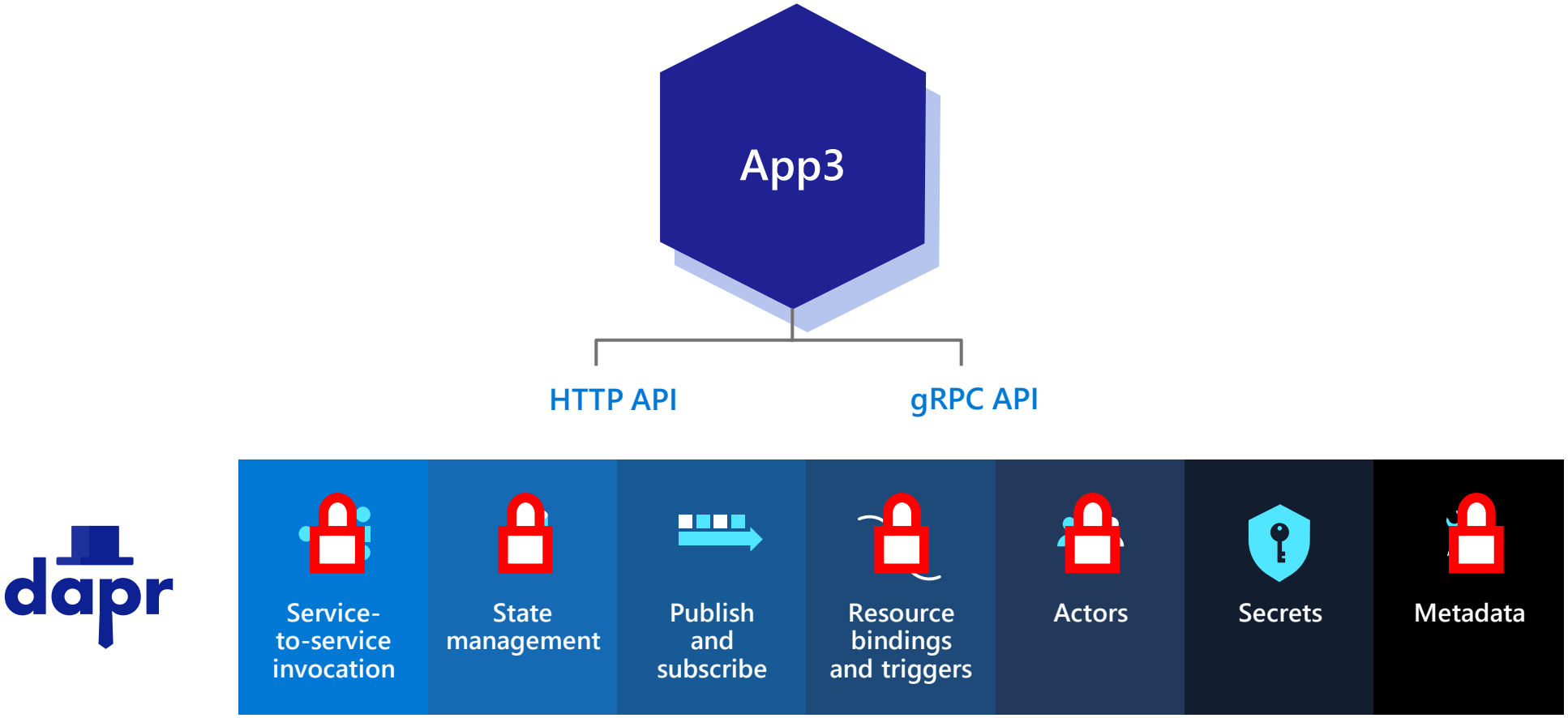
Observability

Überwachung und Messung aller Nachrichtenaufrufe zwischen Dapr-Systemdiensten, Komponenten und Anwendungen

Secrets

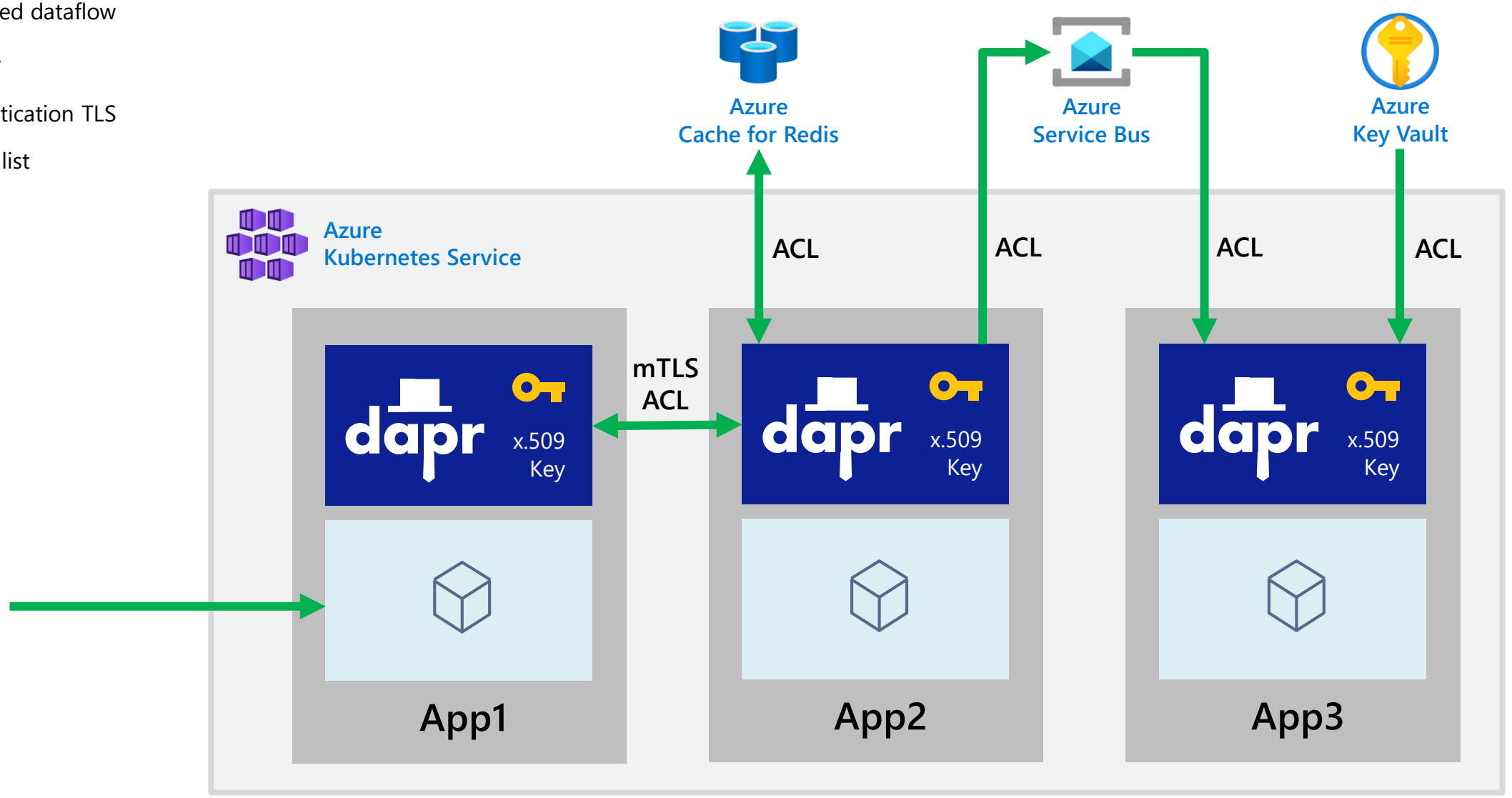
Sicherer Zugriff auf Schlüssel aus der Anwendung heraus

Dapr APIs - ACL



Legend

- explicitly allowed dataflow
- SPIFFE identity
- **mTLS** mutual authentication TLS
- **ACL** access control list



Possible Next Steps

- OAuth endpoint authorization:
  Dapr OAuth 2.0 middleware
- Dapr Sidecar <> Application:
  Trusted security boundary / Token auth
- Denial of service (DOS) protection:
  Dapr rate limiting middleware

Microsoft

Thank you

#SummITup

#SummITup