Data	Highest Impact Level (C/I/A)	Source	Destination	Protocol	Encryption	Authentication	Network route
Example: customer details	*Confidentiality*	*customer*	*Ingress controller*	BCTL responsibility	Not by default - BCTL responsibility	Not by default - BCTL responsibility	*public*
Developer K8s API calls		kubectl	API server	HTTPS	yes		public
Customer details	Confidentiality	Ingress controller	Booking pod	BCTL responsibility	Not by default - BCTL responsibility		cluster-internal
Customer details	Confidentiality	Booking pod	PostgreSQL Pod			Not by default - BCTL responsibility	cluster-internal
Customer details	Confidentiality	PostgreSQL Pod	Persistent storage	AWS responsibility	AWS responsibility	AWS responsibility	
Compliance info		Booking pod	Compliance pod	BCTL responsibility	Not by default - BCTL responsibility	Not by default - BCTL responsibility	
Compliance info		Compliance pod	Government-owned S3 bucket	HTTPS, AWS issued public cert	yes		
Invoicing info	Confidentiality	Invoicing pod	customer				
Poll for new pods		Kubelet	API server	gRPC over TLS	yes	Certificate authentication - self-signed CA	cluster-internal
Poll for services / endpoints			API server	gRPC over TLS	yes	Certificate authentication - self-signed CA	cluster-internal
Get container image		Container runtime		gRPC over TLS	yes	Certificate authentication - self-signed CA	cluster-internal
Read/write state info		API server			yes	Certificate authentication - self-signed CA	cluster-internal
Poll for current / desired state		Controllers		gRPC over TLS	yes	Certificate authentication - self-signed CA	cluster-internal
Poll for new pods / schedule pods			API server	gRPC over TLS	yes	Certificate authentication - self-signed CA	cluster-internal