perplexity

10-Minute Speech on CoCo: Trustee Passport Mode

Introduction

Good morning/afternoon everyone,

Today, I'm going to explain **CoCo**—specifically, the Trustee Passport Mode—in a simple and clear way. Whether you're technical or not, by the end of this talk, you'll understand what CoCo is, why it matters, and how its Trustee Passport Mode works.

What is CoCo?

CoCo stands for **Confidential Containers**. It's a technology that helps run applications in containers while keeping data and processes secure—even from the people who manage the infrastructure.

- **Containers** are like lightweight, portable boxes that hold your applications and everything they need to run.
- **Confidentiality** means that even if someone has access to the computer running your container, they can't see what's inside.

Why Do We Need CoCo?

- **Security:** In cloud computing, your applications might run on computers you don't control. CoCo ensures your data stays private.
- **Trust:** With CoCo, you can prove to others that your application is running in a secure environment.
- **Compliance:** Many regulations require strong data protection, and CoCo helps meet those needs.

The Role of the Trustee

A **Trustee** in CoCo is like a security guard for your confidential containers. It helps:

- **Verify** that only trusted code runs in your containers.
- **Release secrets** (like passwords or encryption keys) only if the environment is secure.

Trustee Modes: BuiltIn, gRPC, and Passport

There are three main ways to set up a Trustee:

1. **BuiltIn Mode:** Simple, but limited to one deployment.
2. **gRPC Mode:** Uses remote procedure calls for more flexibility.
3. **Passport Mode:** The focus of today's talk—enables multiple trustees to work together securely[1].

What is Passport Mode?

Passport Mode allows multiple trustees to operate in the same environment without interfering with each other. This is especially useful when you need more than one trustee for different tasks or organizations.

- **No Operator Dependency:** Unlike older modes, Passport Mode doesn't rely on a central operator that limits you to one trustee.
- **Direct Deployment:** You set up each trustee directly, giving you more control and flexibility.

How Does Trustee Passport Mode Work?

Let's break it down step by step:

1. Key and Certificate Generation

- **Keys and Certificates** are like digital ID cards and signatures.
- You first generate a **Certificate Authority (CA)**—the master key that signs everything else.
- Then, you create **signing keys** and **certificates** for each trustee.
- These are used to sign and verify tokens that prove a container is running securely.

2. Setting Up Trustees

- **Trustee 1** contains the main security services (AS and RVPS).
- **Trustee 2** is set up without those services, but can still verify tokens signed by Trustee 1.

3. Token Verification

- When a container wants access to secrets, it presents a **CoCo attestation token**.
- Trustee 2 checks the token's signature using the agreed-upon keys and certificates.
- If everything matches, Trustee 2 releases the needed resources.

4. Authorization and HTTPS

- Each trustee uses **authorization keys** to ensure only trusted clients can interact.
- **HTTPS certificates** are used to secure all communications, keeping data safe in transit.

5. Configuration

- Each trustee has its own **configuration files** specifying keys, certificates, and settings.
- These files are deployed as Kubernetes secrets and config maps, ensuring they're managed securely.

Key Benefits of Passport Mode

- **Multiple Trustees:** Run several trustees in the same environment without conflicts.
- **Improved Security:** Each trustee can have its own keys and policies.
- **Flexibility:** Organizations can manage their own trustees independently.
- **No Overwriting:** Deploying one trustee won't overwrite another.

Real-World Example

Imagine two companies sharing the same cloud infrastructure. With Passport Mode:

- Each company sets up its own trustee, with its own security rules.
- They can both verify and release secrets independently.
- No risk of one company's trustee interfering with the other's.

Summary Table: Trustee Modes Comparison

Feature	BuiltIn Mode	gRPC Mode	Passport Mode
Operator Dependency	Yes	Yes	No
Multiple Trustees	No	No	Yes
Flexibility	Low	Medium	High
Setup Complexity	Simple	Moderate	Moderate-Advanced

Conclusion

To sum up:

- **CoCo** keeps your containers confidential and secure.
- **Trustee Passport Mode** lets you run multiple, independent trustees, giving you flexibility and strong security.
- With Passport Mode, you're in control—no more limitations from central operators, and no risk of overwriting existing trustees.

Thank you for listening! If you have any questions about CoCo or Trustee Passport Mode, I'm happy to answer them[1].

⁂

1. CoCo-Main-Documentation.pdf