# SROS use case intro and project overview

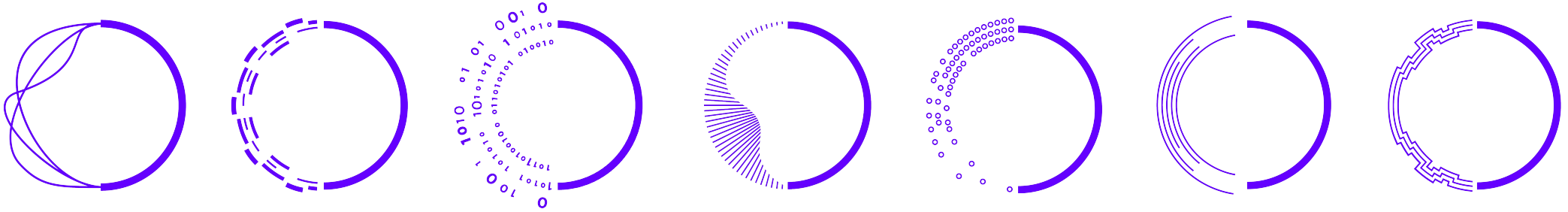
**ROS2 Security Workgroup presentation**

**Secure Systems Research Centre (SSRC)**

**11th May 2021**

# Research areas

Technology Innovation Institute



**QUANTUM RESEARCH CENTRE**

**AUTONOMOUS ROBOTICS RESEARCH CENTRE**

**CRYPTOGRAPHY RESEARCH CENTRE**

**ADVANCED MATERIALS RESEARCH CENTRE**

**DIGITAL SECURITY RESEARCH CENTRE**

**DIRECTED ENERGY RESEARCH CENTRE**

**SECURE SYSTEMS RESEARCH CENTRE**

EL2 Communities:

Hardware Hardening Against Tampering, Alternative Channels Resilience (Platforms)

Software Hardening & Resilience Against Malware (OS, Apps, Cloud)

Maintaining System Integrity & Preventing Data Exfiltration

Communication Hardening Protocols, Alternative Networks Resilience

Secure & Resilient Cloud Infrastructure

Secure & Resilient Platforms (Vehicles, Phones)

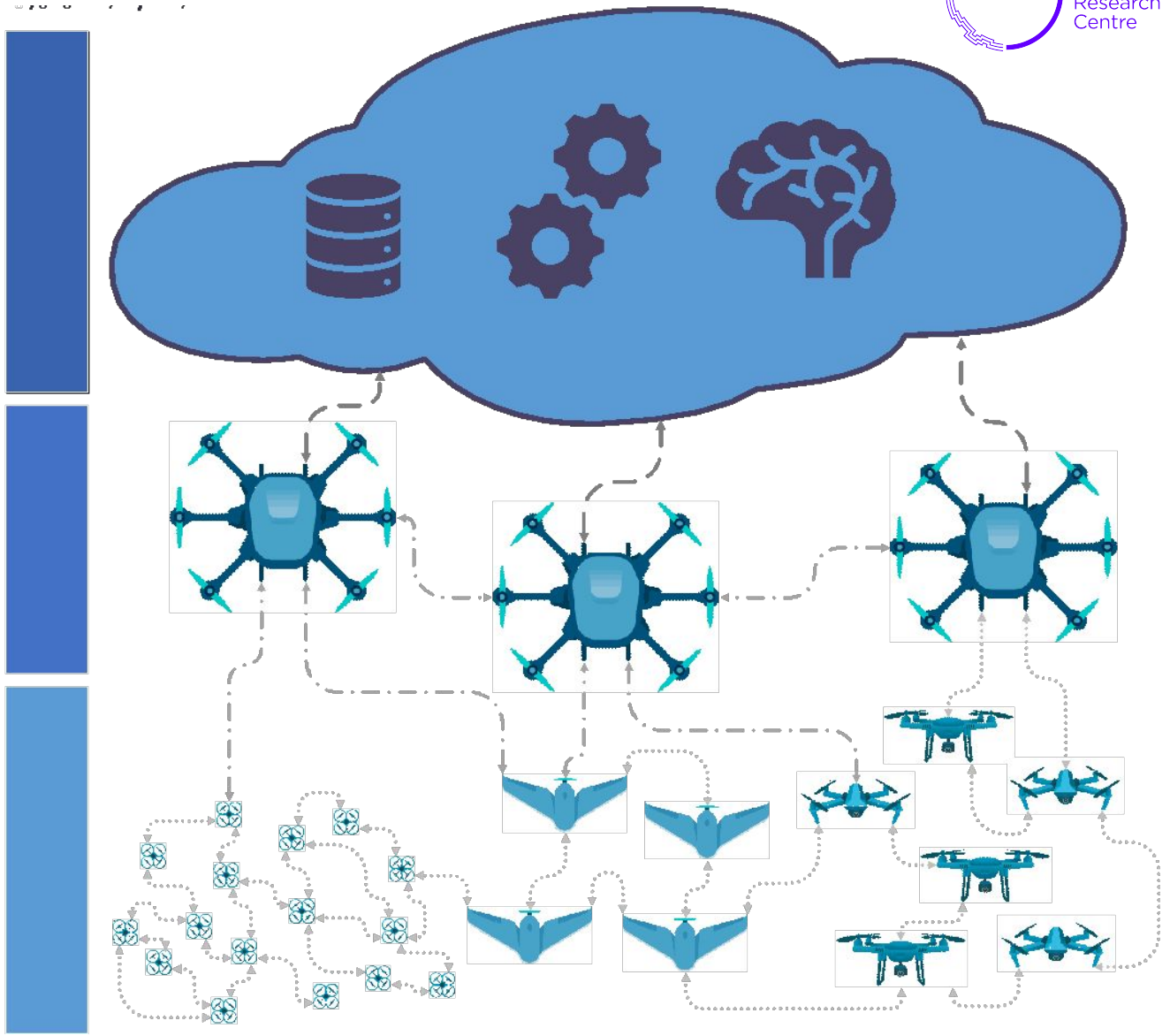
Secure & Resilient Communications

# Secure Systems Research Centre

# Secure Autonomous Systems

Only E2E Security and Resilience makes these Secure Autonomous Use Cases involving logistics and surveillance use possible

- Secure delivery systems (e.g., vaccines)
- Burning Building Connectivity to IOT and Smartphones
- Emergency Response – Infrastructure-on-Fly (e.g., Earthquake)
- Ground Pipeline Monitoring and Control
- Underwater Monitoring



Secure Systems Research Centre

PURDUE UNIVERSITY

Georgia Tech

Tampere University

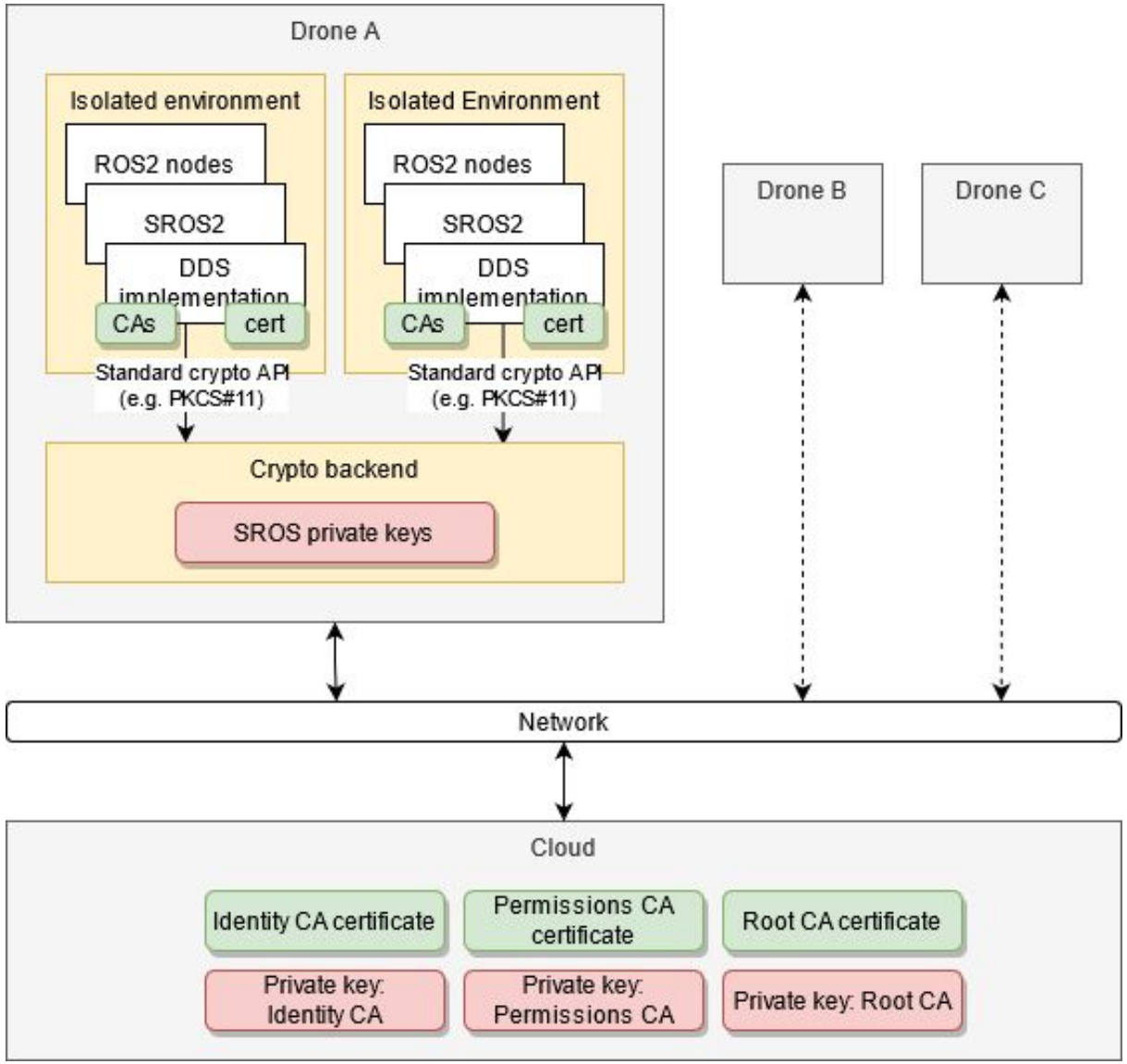
Scuola universitaria professionale della Svizzera italiana

SUPSI

# Drone architecture in ROS2 context

Secure Systems Research Centre

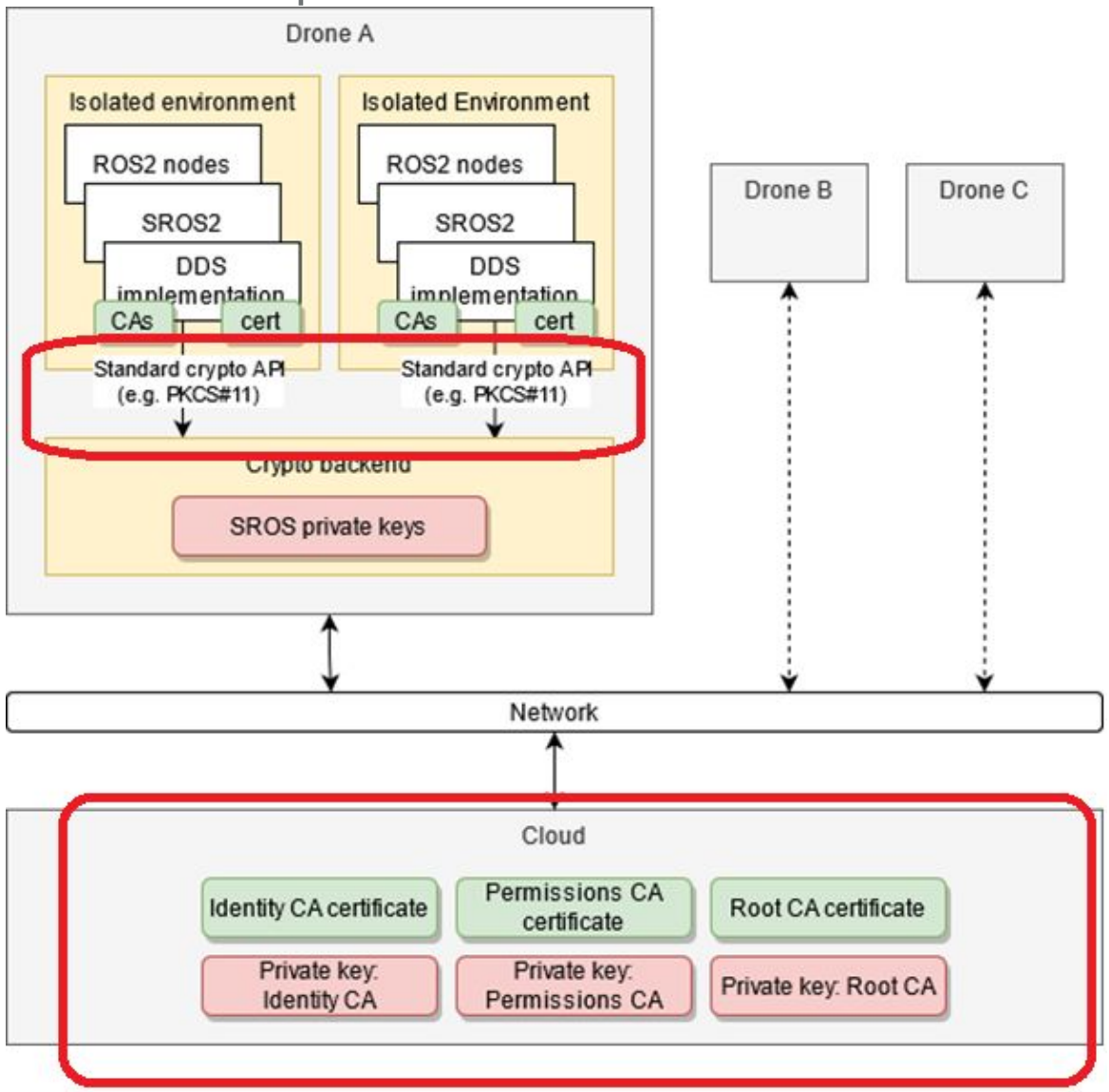
- Currently using ROS2 Foxy and fastRTPS 2.0.2
- Each drone runs ROS2 nodes in isolated environments
- ROS2 nodes communicate **inside and between** drones
- Crypto backend: a special environment that will not have ROS two nodes running. It works as an enclave to store the cryptographic keys. These keys never leave the enclave.
- Cloud acts as the root of trust. Root CA and intermediate CAs reside in the cloud.
- The signed ACLs (permissions) and environment's identity cert can be uploaded to a drone during provisioning and configuration updates.



# Open issues with current SROS setup

There are two identified issues for us to tackle with our SROS setup

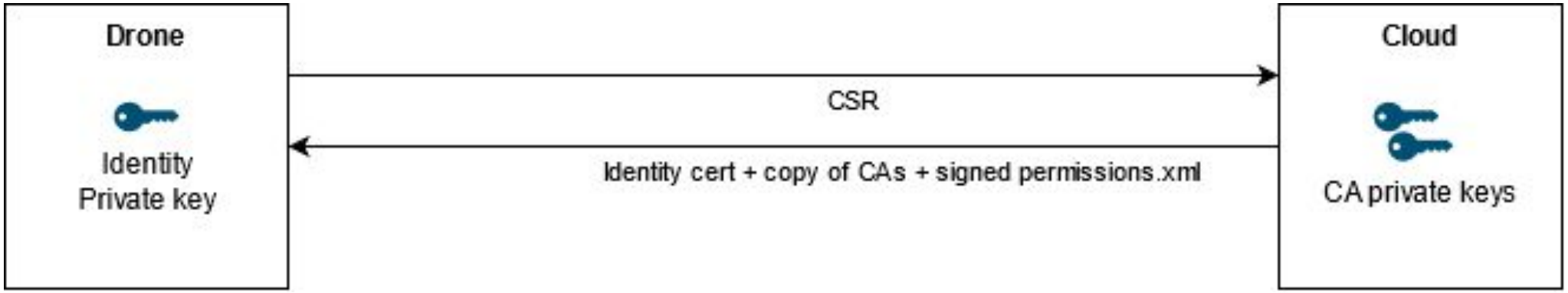
1. Use of centralized PKI solution
2. Consume the identity keys that are stored in an enclave



# Use Case: External CA

Secure Systems Research Centre

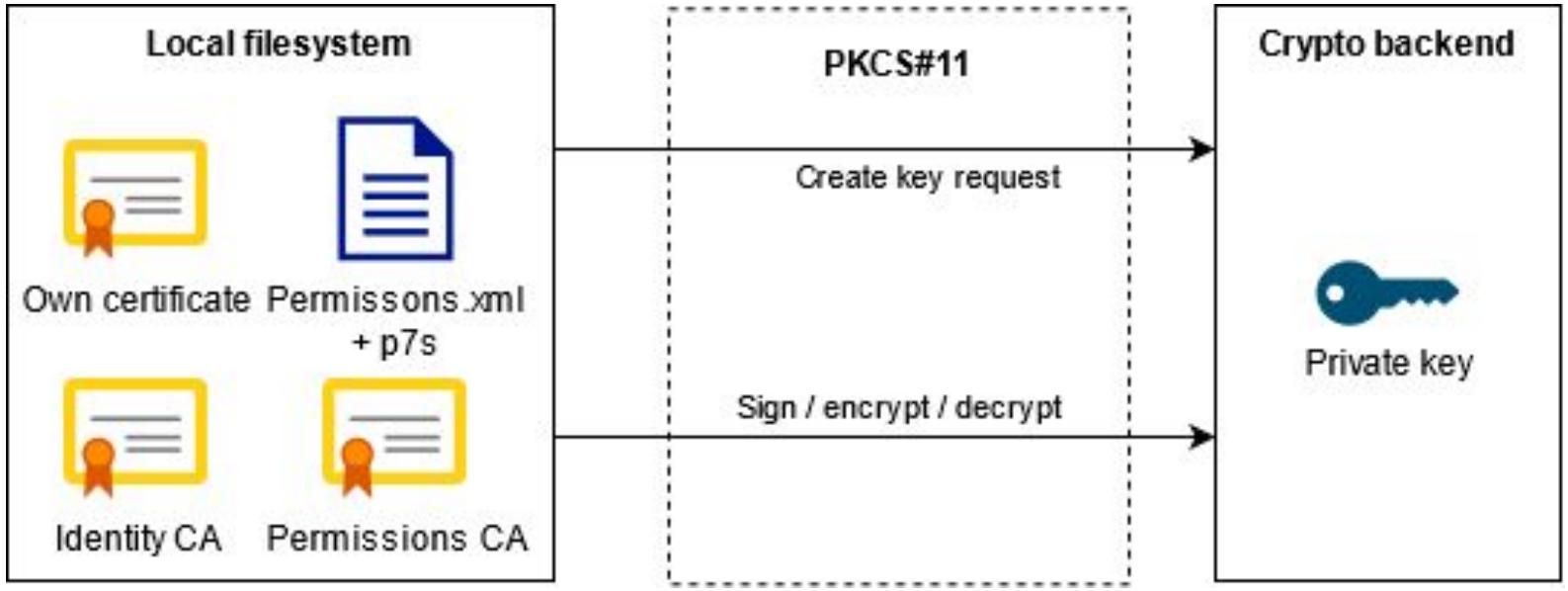
- CA and intermediate CAs on the cloud
- Drone components to generate their own key pairs (on the enclave)
- Drone components to generate the Certificate Signing Request (CSR) for their own authentication certificates
  - Copy-pasting the CSRs from drones to the cloud manually or part of existing provisioning data flows is OK
- Sign drones' authentication certificates on the cloud using Identity CA.
- Sign permissions on the cloud using Permissions CA
- Copy the signed auth certificates, signed ACL and CA certs back to the drone
- Next steps: certificate revocation & revocation lists

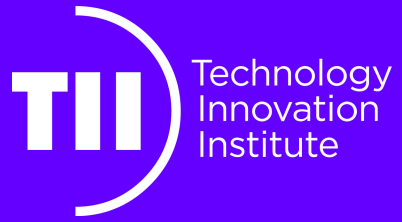


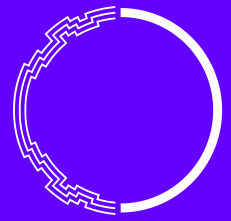
# Use Case: Key protection with an enclave

Secure Systems Research Centre

- VM's private key to reside on the enclave and to be consumer over an API so that they key never leaves the enclave (e.g. PKCS#11)
- Public components (e.g. the authentication certificates and CA files) are OK and preferred to stay in the local file system as they are today.





Secure
Systems
Research
Centre

tii.ae