Smart Cities R5 Test

Introduction

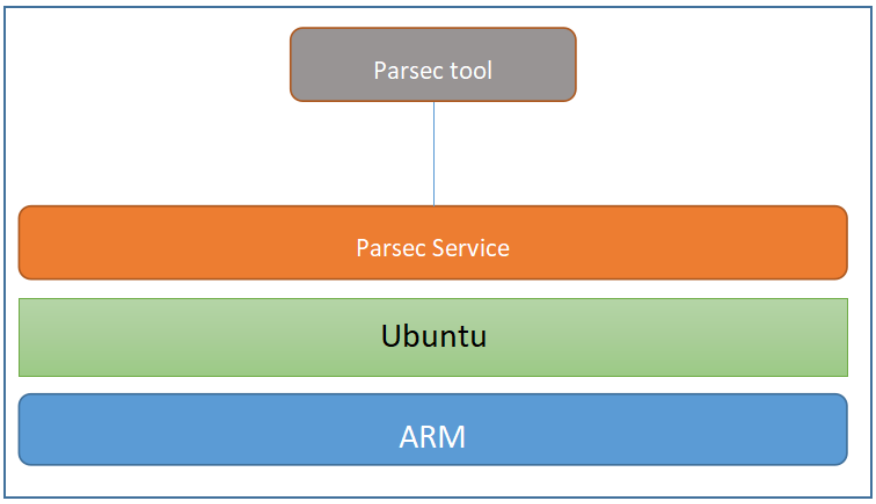
This document covers Test Deployment Environment and Test Case Result for PARSEC on Smart Cities Blueprint.

Akarino Test Group Information

N/A

Overall Test Architecture

Parsec Service and Parsec tool are Installed on the same machine. Use Parsec tool to connect and test Parsec server.



Software Version

Ubuntu 18.04 LTS

parsec-service 0.8.0

parsec-tool 0.3.1

Devices Under Test

Amazon AWS ARM64 servers

CPU: Model name: Neoverse-N1

CPU(s): 2

BogoMIPS: 243.75

Mem: 8Gb

Parsec Service Unit Test

1.Start Parsec Service

cd cassini/smartcities/parsec

cargo build --release --features "mbed-crypto-provider,direct-authenticator"

RUST_LOG=info ./target/release/parsec -c e2e_tests/provider_cfg/mbed-crypto/config.toml

2.Config parsec.sock path

export PARSEC_SERVICE_ENDPOINT=unix:/tmp/parsec.sock

3.Start Unit test

cd e2e_tests

cargo test --features mbed-crypto-provider normal_tests

4.Test result

running 125 tests

test per_provider::normal_tests::aead::aead_encrypt_ccm_decrypt ... ok

test per_provider::normal_tests::aead::aead_encrypt_ccm_decrypt_not_equal ... ok

test per_provider::normal_tests::aead::aead_encrypt_ccm_encrypt ... ok

test per_provider::normal_tests::aead::aead_encrypt_ccm_encrypt_decrypt ... ok

test per_provider::normal_tests::aead::aead_encrypt_ccm_encrypt_not_equal ... ok

test per_provider::normal_tests::aead::aead_not_supported ... ok

test per_provider::normal_tests::aead::simple_aead_encrypt_ccm ... ok

test per_provider::normal_tests::asym_encryption::asym_decrypt_no_key ... ok

test per_provider::normal_tests::asym_encryption::asym_decrypt_not_permitted ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_and_decrypt_rsa_pkcs ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_decrypt_rsa_pkcs_different_keys ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_no_key ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_not_permitted ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_not_supported ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_verify_decrypt_with_rsa_crate ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_verify_decrypt_with_rsa_crate_oaep ... ok

test per_provider::normal_tests::asym_encryption::asym_encrypt_wrong_algorithm ... ok

test per_provider::normal_tests::asym_encryption::asym_verify_decrypt_with_internet ... ok

test per_provider::normal_tests::asym_encryption::simple_asym_decrypt_oaep_with_salt ... ok

test per_provider::normal_tests::asym_encryption::simple_asym_encrypt_rsa_oaep ... ok

test per_provider::normal_tests::asym_encryption::simple_asym_encrypt_rsa_pkcs ... ok

test per_provider::normal_tests::asym_sign_verify::asym_sign_and_verify_rsa_pkcs ... ok

test per_provider::normal_tests::asym_sign_verify::asym_sign_no_key ... ok

test per_provider::normal_tests::asym_sign_verify::asym_verify_fail_ecc_sha256 ... ok

test per_provider::normal_tests::asym_sign_verify::asym_verify_no_key ... ok

test per_provider::normal_tests::asym_sign_verify::asym_verify_with_rsa_crate ... ok

test per_provider::normal_tests::asym_sign_verify::fail_verify_hash2_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::fail_verify_hash2_rsa ... ok

test per_provider::normal_tests::asym_sign_verify::fail_verify_hash_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::fail_verify_hash_rsa ... ok

test per_provider::normal_tests::asym_sign_verify::only_verify_from_internet ... ok

test per_provider::normal_tests::asym_sign_verify::private_sign_public_verify ... ok

test per_provider::normal_tests::asym_sign_verify::sign_hash_bad_format_rsa_sha256 ... ok

test per_provider::normal_tests::asym_sign_verify::sign_hash_not_permitted ... ok

test per_provider::normal_tests::asym_sign_verify::sign_hash_not_permitted_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::sign_message_not_permitted ... ok

test per_provider::normal_tests::asym_sign_verify::sign_verify_hash_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::sign_verify_message_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::simple_sign_hash_ecdsa_sha256 ... ok

test per_provider::normal_tests::asym_sign_verify::simple_sign_hash_rsa_sha256 ... ok

test per_provider::normal_tests::asym_sign_verify::simple_verify_hash_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::simple_verify_hash_rsa ... ok

test per_provider::normal_tests::asym_sign_verify::verify_ecc_with_ring ... ok

test per_provider::normal_tests::asym_sign_verify::verify_hash_bad_format_rsa ... ok

test per_provider::normal_tests::asym_sign_verify::verify_hash_not_permitted_ecc ... ok

test per_provider::normal_tests::asym_sign_verify::verify_hash_not_permitted_rsa ... ok

test per_provider::normal_tests::asym_sign_verify::verify_message_not_permitted ... ok

test per_provider::normal_tests::asym_sign_verify::verify_with_ring ... ok

test per_provider::normal_tests::auth::delete_wrong_key ... ok

test per_provider::normal_tests::auth::two_auths_same_key_name ... ok

test per_provider::normal_tests::basic::authenticator_not_registered ... ok

test per_provider::normal_tests::basic::flags_ignored ... ok

test per_provider::normal_tests::basic::invalid_accept_type ... ok

test per_provider::normal_tests::basic::invalid_auth_len ... ok

test per_provider::normal_tests::basic::invalid_authenticator ... ok

test per_provider::normal_tests::basic::invalid_body_len ... ok

test per_provider::normal_tests::basic::invalid_content_type ... ok

test per_provider::normal_tests::basic::invalid_opcode ... ok

test per_provider::normal_tests::basic::invalid_provider ... ok

test per_provider::normal_tests::basic::reserved_fields_not_zero1 ... ok

test per_provider::normal_tests::basic::reserved_fields_not_zero2 ... ok

test per_provider::normal_tests::basic::status_ignored ... ok

test per_provider::normal_tests::create_destroy_key::create_and_destroy ... ok

test per_provider::normal_tests::create_destroy_key::create_and_destroy_ecc ... ok

test per_provider::normal_tests::create_destroy_key::create_destroy_and_operation ... ok

test per_provider::normal_tests::create_destroy_key::create_destroy_twice ... ok

test per_provider::normal_tests::create_destroy_key::create_twice ... ok

test per_provider::normal_tests::create_destroy_key::destroy_without_create ... ok

test per_provider::normal_tests::create_destroy_key::failed_created_key_should_be_removed ... ok

test per_provider::normal_tests::create_destroy_key::generate_public_rsa_check_modulus ... ok

test per_provider::normal_tests::export_key::check_export_ecc_not_possible ... ok

test per_provider::normal_tests::export_key::check_export_rsa_not_possible ... ok

test per_provider::normal_tests::export_key::check_export_rsa_possible ... ok

test per_provider::normal_tests::export_key::check_rsa_export_format ... ok

test per_provider::normal_tests::export_key::export_ecc_private_key ... ok

test per_provider::normal_tests::export_key::export_key ... ok

test per_provider::normal_tests::export_key::export_key_not_supported ... ok

test per_provider::normal_tests::export_key::export_rsa_private_key_matches_import ... ok

test per_provider::normal_tests::export_key::export_without_create ... ok

test per_provider::normal_tests::export_key::import_and_export_ecc_public_key_by_export_key_fn ... ok

test per_provider::normal_tests::export_key::import_and_export_rsa_public_key ... ok

test per_provider::normal_tests::export_public_key::check_export_ecc_public_possible ... ok

test per_provider::normal_tests::export_public_key::check_export_rsa_public_possible ... ok

test per_provider::normal_tests::export_public_key::check_public_ecc_export_format ... ok

test per_provider::normal_tests::export_public_key::check_public_ecc_export_format2 ... ok

test per_provider::normal_tests::export_public_key::check_public_rsa_export_format ... ok

test per_provider::normal_tests::export_public_key::export_ecc_public_key ... ok

test per_provider::normal_tests::export_public_key::export_rsa_public_key ... ok

test per_provider::normal_tests::export_public_key::export_without_create ... ok

test per_provider::normal_tests::export_public_key::import_and_export_ecc_public_key ... ok

test per_provider::normal_tests::export_public_key::import_and_export_ecc_public_key_by_export_public_key_fn ... ok

test per_provider::normal_tests::export_public_key::import_and_export_rsa_public_key ... ok

test per_provider::normal_tests::generate_random::generate_random_not_supported ... ok

test per_provider::normal_tests::generate_random::generate_zero_bytes ... ok

test per_provider::normal_tests::generate_random::simple_generate_random ... ok

test per_provider::normal_tests::hash::hash_compare_false ... ok

test per_provider::normal_tests::hash::hash_compare_ripe_md160 ... ok

test per_provider::normal_tests::hash::hash_compare_sha256 ... ok

test per_provider::normal_tests::hash::hash_compare_sha512 ... ok

test per_provider::normal_tests::hash::hash_compute_ripe_md160 ... ok

test per_provider::normal_tests::hash::hash_compute_sha256 ... ok

test per_provider::normal_tests::hash::hash_compute_sha512 ... ok

test per_provider::normal_tests::hash::hash_not_supported ... ok

test per_provider::normal_tests::import_key::check_format_import1 ... ok

test per_provider::normal_tests::import_key::check_format_import2 ... ok

test per_provider::normal_tests::import_key::check_format_import3 ... ok

test per_provider::normal_tests::import_key::create_and_import_ecc_key ... ok

test per_provider::normal_tests::import_key::create_and_import_rsa_key ... ok

test per_provider::normal_tests::import_key::failed_imported_key_should_be_removed ... ok

test per_provider::normal_tests::import_key::import_ecc_key ... ok

test per_provider::normal_tests::import_key::import_ecc_key_twice ... ok

test per_provider::normal_tests::import_key::import_ecc_private_key ... ok

test per_provider::normal_tests::import_key::import_rsa_key ... ok

test per_provider::normal_tests::import_key::import_rsa_key_twice ... ok

test per_provider::normal_tests::key_agreement::key_agreement_not_supported ... ok

test per_provider::normal_tests::key_agreement::raw_key_agreement_brainpoolpr1 ... ok

test per_provider::normal_tests::key_agreement::raw_key_agreement_secpr1 ... ok

test per_provider::normal_tests::key_agreement::raw_key_agreement_two_generated_parties ... ok

test per_provider::normal_tests::key_agreement::simple_raw_key_agreement ... ok

test per_provider::normal_tests::key_attributes::no_usage_flag_set ... ok

test per_provider::normal_tests::key_attributes::wrong_permitted_algorithm ... ok

test per_provider::normal_tests::key_attributes::wrong_type ... ignored

test per_provider::normal_tests::key_attributes::wrong_usage_flags ... ok

test per_provider::normal_tests::ping::mangled_ping ... ok

test per_provider::normal_tests::ping::test_ping ... ok

test result: ok. 124 passed; 0 failed; 1 ignored; 0 measured; 31 filtered out; finished in 14.21s

Parsec Tool Test

1.Keep Parsec Service running

2.Build Parsec Tool

git clone https://github.com/parallaxsecond/parsec-tool.git

cd parsec-tool

cargo build

3.Set Parsec socket path

export PARSEC_SERVICE_ENDPOINT=unix:/tmp/parsec.sock

4.Test Ping

./target/debug/parsec-tool ping

[INFO] Service wire protocol version

1.0

5.Test list-providers

./target/debug/parsec-tool list-providers

[INFO] Available providers:

ID: 0x01 (Mbed Crypto provider)

Description: User space software provider, based on Mbed Crypto - the reference implementation of the PSA crypto API

Version: 0.1.0

Vendor: Arm

UUID: 1c1139dc-ad7c-47dc-ad6b-db6fdb466552

ID: 0x00 (Core provider)

Description: Software provider that implements only administrative (i.e. no cryptographic) operations

Version: 0.8.0

Vendor: Unspecified

UUID: 47049873-2a43-4845-9d72-831eab668784

6.Test create key

./target/debug/parsec-tool create-ecc-key -k Jack

[INFO] Creating ECC key...

[INFO] Key "Jack" created.

7.Test list key

./target/debug/parsec-tool list-keys

[INFO] Available keys:

* Jack (Mbed Crypto provider, EccKeyPair { curve_family: SecpR1 }, 256 bits, permitted algorithm: AsymmetricSignature(Ecdsa { hash_alg: Specific (Sha256) }))

8.Test sign with key

./target/debug/parsec-tool sign -k Jack "This is Parsec Sign!"

[INFO] Hashing data with Sha256...

[INFO] Signing data with Ecdsa { hash_alg: Specific(Sha256) }...

MEQCIAlQjPyGuQ4d3KRT1m9RMJaKacn0wBnHaQQxFSZm3lQuAiBjQZqO6ofdfCwOeQCPhk4/lwuOFANKE2Ek/xEiBeruFg==

9.Test export public key

./target/debug/parsec-tool export-public-key -k Jack

-----BEGIN PUBLIC KEY-----

BOH0eSSx72xRLXBa6jAGIaq9EIV0ufRKdOz41C8R1DSV8Bi1AkXbNrkYhOKTMV6X

S4GwiXgSThdHlPl01bsaHwM=

-----END PUBLIC KEY-----

10.Test delete key

./target/debug/parsec-tool delete-key -k Jack

[INFO] Deleting a key...

[INFO] Key "Jack" deleted.

Test Dashboards

Single pane view of how the test score looks like for the Blue print.

Total Tests	Test Executed	Pass	Fail	In Progress
1	1	1	0	0

Additional Testing

N/A

Bottlenecks/Errata

N/A