Themis

A single library for building strong consistent data security across all platforms.

COSSACK LABS

Essential benefits for:

- **Your clients:** protected data in storage and in transit.
- **Your developers**: pre-baked data protection scenarios.
- **Your product**: consistent compatible data security across all platforms.

Languages and platforms:

- **Core library:** C/C++
- **Mobile:** iOS (Swift, Objective-C), Android (Java).
- **Regular:** Ruby, Python, NodeJS, Go, Java, PHP.
- **OS**: Linux (x86/ARM), macOS, iOS, Android.
- **Ports**: Chrome, Redis, PostgreSQL.

Key features:

- **Pre-baked** blocks for solving everyday use cases.
- **Unified API** across many languages and platforms.
- Secure-by-default and **misuse-proof.**
- Requires minimum cryptographic knowledge to implement in-app security.
- Built on industry-recognized cryptographic primitives.

License: free, Apache 2 license.

Support contracts available depending on your use case.

Overview

Implementing cryptography in customer applications is often hard. Choosing cipher suites, defining key lengths, and designing key exchange schemes require plenty of particular competences and lead to mistakes when done by applied developers.

Themis is an open-source **high-level cryptographic services library** for mobile and server platforms that provides secure data exchange, authentication, and storage protection. Themis provides **ready-made building components**, which simplify usage of core cryptographic security operations.

Themis brings a unified cryptographic security across multiple platforms and is suitable for building sophisticated data security systems. We are using Themis as a core library for our other security products.

Themis contains **4 core cryptographic systems**:

- **Secure Cell**: multi-mode symmetric container.
- **Secure Message**: general-purpose asymmetric cryptographic primitive.
- **Secure Session**: session-oriented, forward secrecy datagram exchange solution.
- **Secure Comparator**: SMP-based Zero-Knowledge Protocol for authentication.

The core crypto systems of Themis meet most of the needs modern applications have towards data security:

- **Secure storage**: protecting data to be stored or transmitted using a symmetric secret.
- **Secure envelope:** public key container for exchanging messages between two parties and binding the access to private keys instead of secrets.
- **Secure network exchange**: protecting sequential network exchanges (API, sessions, chats, sockets) with specially designed lightweight protocol.
- **Zero-leakage authentication**: Zero-knowledge-based scheme for authentication and handling requests that contain sensitive data, without exposing secrets to the network.

Themis

A single library for building strong consistent data security across all platforms.

COSSACK LABS

Secure Cell

Secure Cell provides the means for protection of the stored data, such as database records or filesystem files. Secure Cell provides symmetric encryption with **AES256** in **GCM** and **CTR** modes.

Secure Cell can be used in 3 different modes:

- **Seal mode** provides the strongest secure guarantees and prevents data tampering.
- **Token protect mode** is length-preserving — encrypted objects don't change lengths, yet their authentication data has to be stored elsewhere.
- **Context imprint mode** is a length-preserving mode that contains no authentication tag data.

Secure Cell comes with an **embedded key derivation function (KDF)** so you can use your normal password as an argument.

Secure Session

Secure Session is a sequence dependent, stateful messaging session system. It works best for P2P communication with preserved session state, i.e. sockets or API sessions. It is **protocol-agnostic** and operates on the 5th layer of the OSI model.

Secure Session is **lightweight**, easy to use and features:

- secure end-to-end communication with perfect forward secrecy & replay protection;
- strong mutual peer authentication;
- low negotiation round-trip;
- strong encryption (ECC + AES);
- straightforward integration process.

Secure Session is stateful and requires session negotiation before data exchange. **Session negotiation** is carried out via **ECDH** with additional security measures against MitM. **Data exchange** is a process of encrypting source data into datagram and sending it to a remote party.

Secure Session can be used via callback API or buffer-aware ("data only") API methodology.

Secure Message

Secure Message provides a simple way to protect your messages and bind them to the credentials of communicating peers using strong cryptography. It adds confidentiality, integrity, and authenticity to your message in one shot (as a stateless single function call).

To encrypt the payload, Secure Message uses Secure Cell primitive. Secure Message can work in **signature** and **encryption** modes.

Cryptographic primitives used:

Mode	Crypto stack
Elliptic Curve: sign	NIST P-256 + Secure Cell
Elliptic Curve: encrypt	NIST P-256 + Secure Cell
RSA: sign	RSA + PKCS#7 + Secure Cell
RSA: encrypt	RSA + PSS + PKCS#7

Secure Comparator

Secure Comparator allows the parties to prove that they both share some secret — a password, a secret request identifier, or any other verification data:

- **zero data is leaked**: no data which could enable to reconstruct/replay the secret is transmitted;
- **protection against dishonest verifiers**: a verifier can't collect sufficient data to reuse it for further authentication.

Cryptographic primitives used:

Core protocol	Socialist Millionaire's Protocol
Computations	Armoured ed25519
Hash	SHA-256