



# encrypt

A scalable and practical  
privacy-preserving framework

## Trusted Execution Environment (TEE)

### TEE-Based Privacy-Preserving Deployment in ENCRYPT

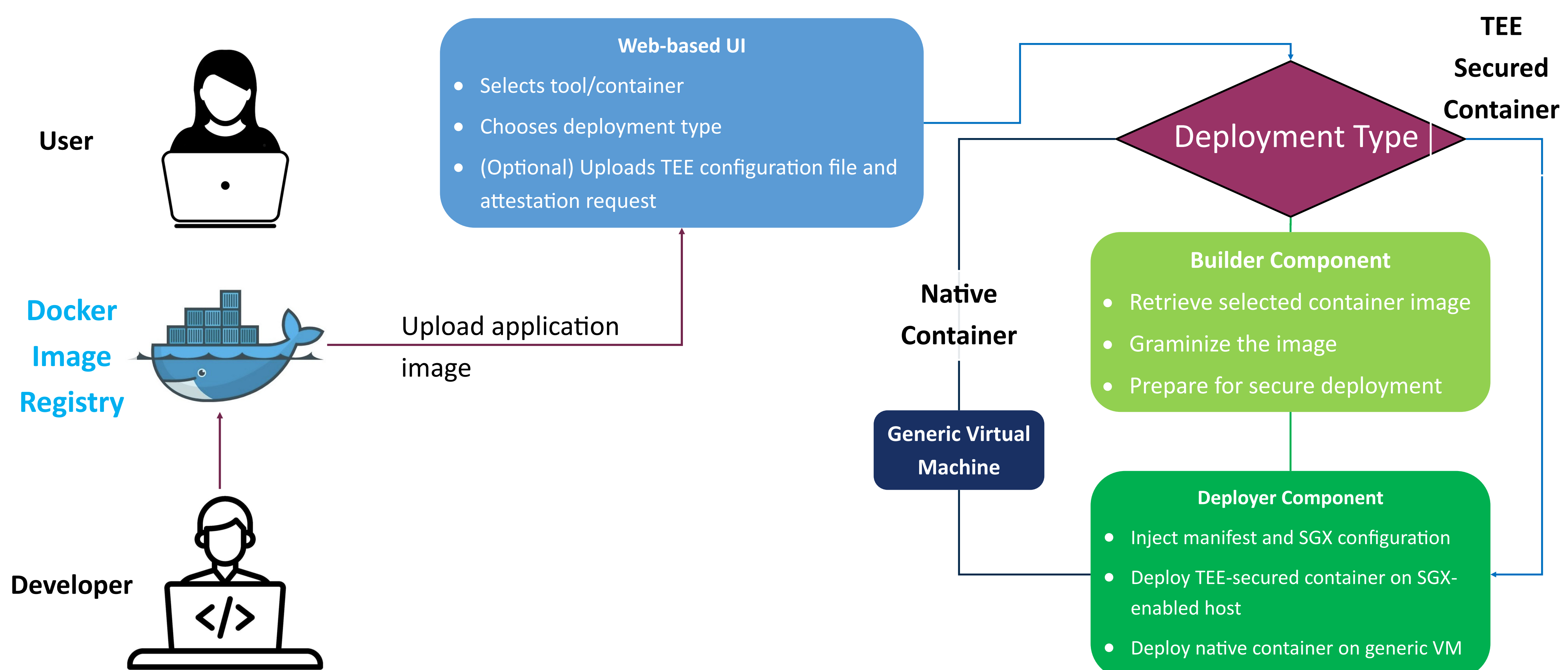
#### OBJECTIVES



- TEEs provide hardware-based security against privileged attackers
- Intel SGX enclaves ensure confidentiality and integrity of code/data, even with full system compromise
- ENCRYPT implements a container-based workflow for secure, privacy-preserving deployments in sensitive domains

**Goal:** Enable user-friendly, secure execution of tools via TEEs with minimal user burden

Type	Tech Used	Pros	Cons
Fair TEE	Gramine SGX runtime	Easy setup, no code changes	Larger TCB, lower security
High TEE	Intel SGX SDK	Smaller TCB, high isolation	Complex setup
Super TEE	SGX SDK + WebAssembly	Two-way sandboxing, full isolation	Resource-heavy



Funded by  
the European Union

This work is supported by the European Union's Horizon Europe programme under grant agreement No 101070670.

**Disclaimer:** Views and opinions expressed are those of the ENCRYPT consortium authors only and do not necessarily reflect those of the European Union or its delegated Agency DG CNECT. Neither the European Union nor the granting authority can be held responsible for them.