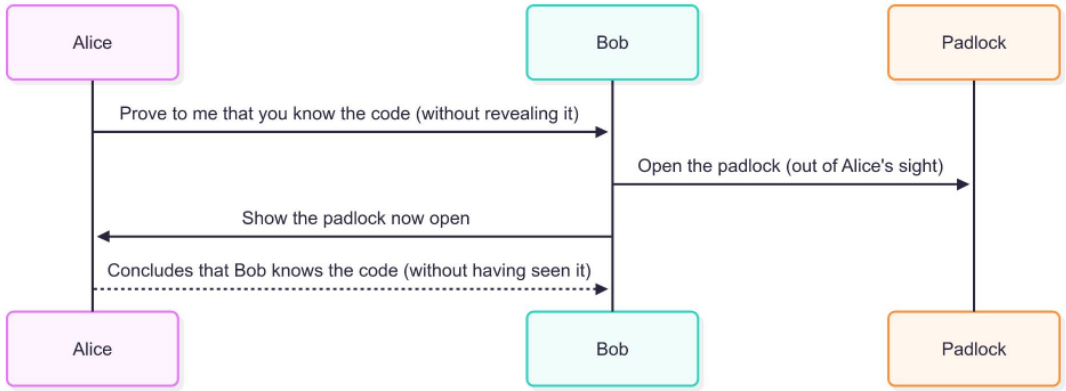
Zero-Knowledge Identity Verification

27 JUIN 2025

auguste.charpentier - quentin.rataud
remy.le-bohec - raphael.gonon

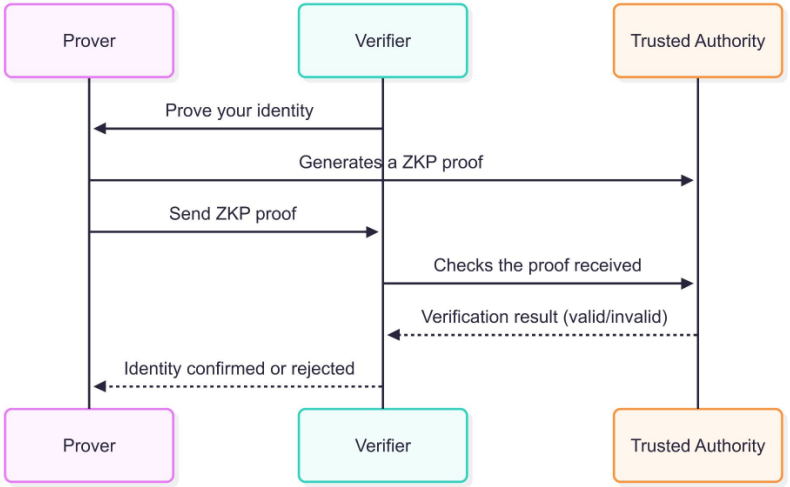
ZKP Basics

A **Zero Knowledge Proof** (ZKP) is a cryptographic protocol that enables one party (the prover) to convince another party (the verifier) of the validity of a statement **without revealing any additional information** beyond the statement's truthfulness.



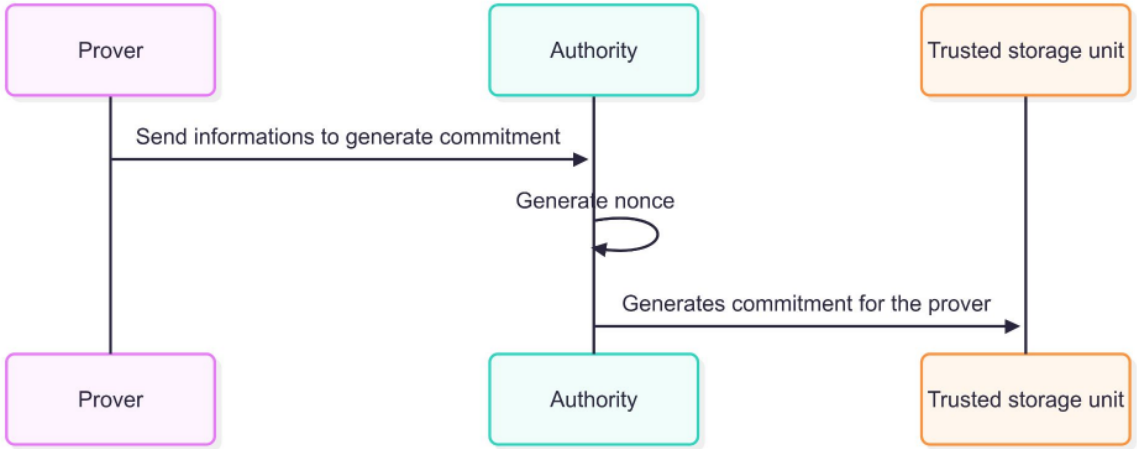
Zero-Knowledge Identity Verification Basics

The aim is to use the ZKP principle to **verify identity attributes** against specific constraints **without revealing them**. This ensures that user data is not exposed to anyone.

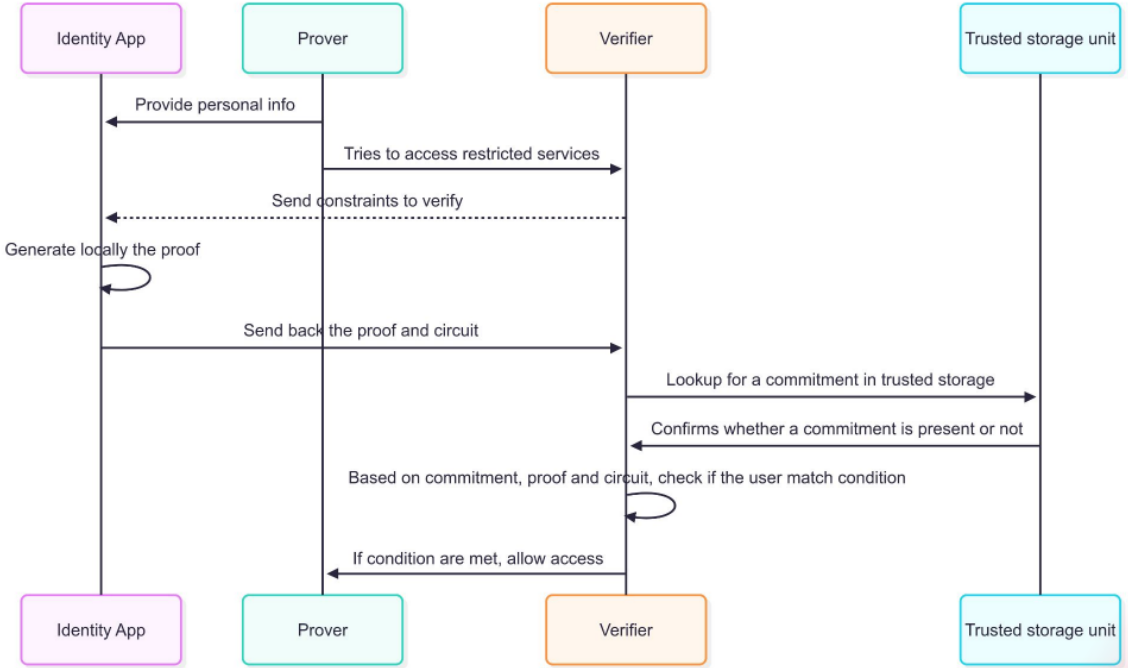


Our implementation

Authority side



Our implementation
Verifier side



Zero-Knowledge Identity Verification

Let's move on to the demo !

Thank you for listening!

If you have any questions, we'll be delighted to answer them.