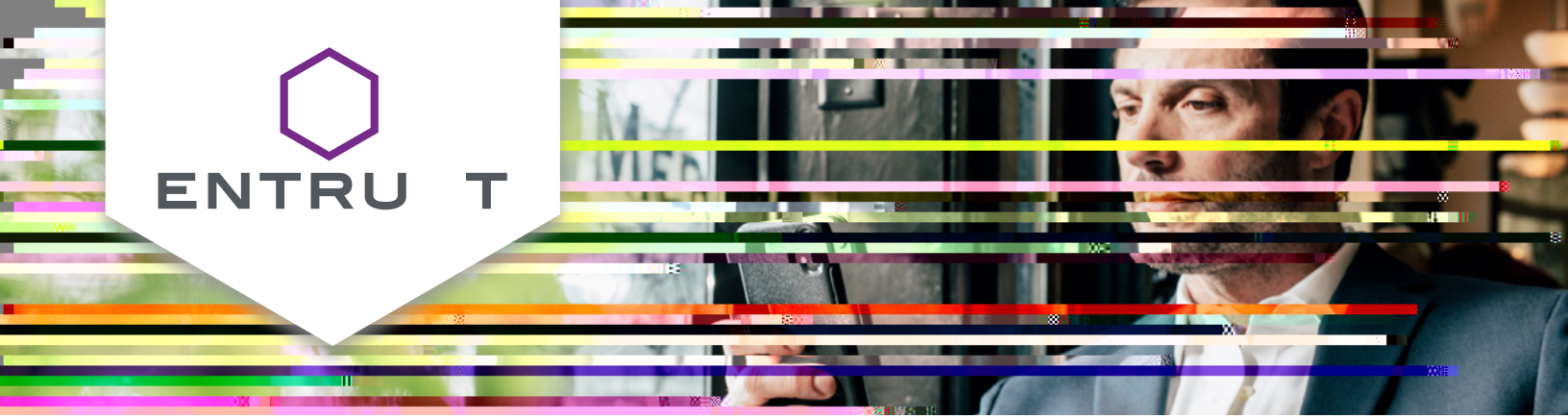

ENTRU T

Entrust Remote Signing Server

HOW IT WORKS

Operation

Entrust Remote Signing Server acts as a server-based signature provider, allowing users to authenticate in order to activate their keys and authorize the signature of documents or document hashes.

Electronic signature provider (eSigP)

PKI material for enrolled users is managed as identity attributes in a secure HSM-based repository. Each user can have one or more digital certificates to sign documents remotely once authenticated.

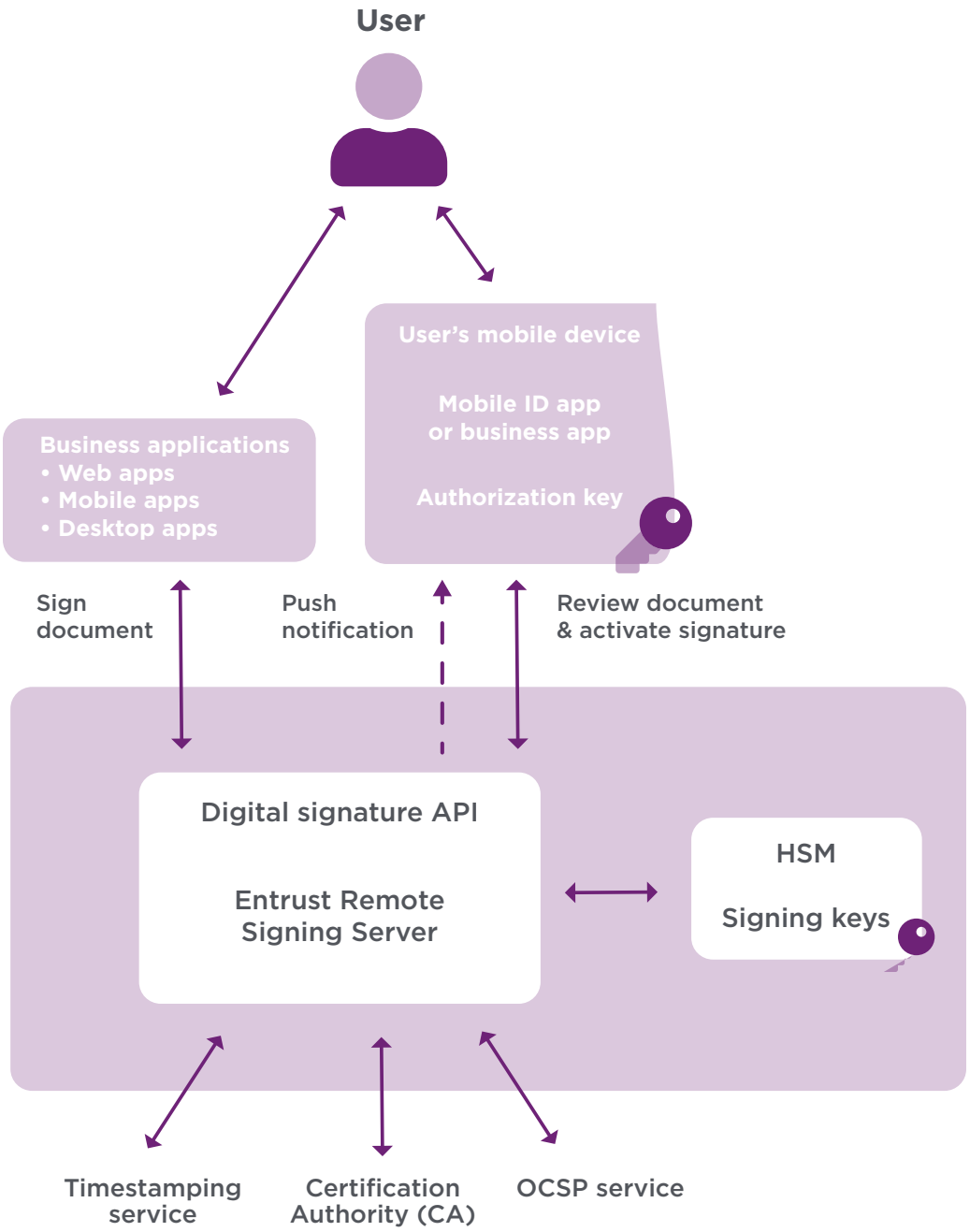
Signing functions are available through a web API or optionally via the Entrust Remote Signing Server Desktop Virtual Card (VC) component.

Identity Two

Entrust Remote Signing Server

Architecture

Entrust Remote Signing Server provides remote signing and 2FA-based signature activation options via web services operated by a Trust Service Provider. The following figure illustrates the interactions between Entrust Remote Signing Server, the optional Mobile ID module, and your infrastructure – the IdP is not represented:



Entrust Remote Signing Server

TECHNICAL SPECIFICATIONS AND REQUIREMENTS

Format:

- Vi t [illegible]