



Alice

contract User
owner = Alice

claimKeyBundle(Bob)

bisemSignal(Bob)

Bob.opkNext()

updateTimestamp()
bisemProtected

emit keyBundleClaimed(...)

contract User
owner = Bob

opkNext()

kontrola omezení

Alice.updateTimestamp()

return opkStoreOffset + 1

Alice požádá
Boba o klíče

Bob vyžádá u Alice
aktualizaci časového
razítka

Bob vrátí index na
zarezerovaný klíč

Alice naslouchá
na událost