MTAT.03.323 Seminar on Blockchain Technology Implementation Project Presentation

GIT - KSI

Developers: arachnid42 team
- Kyrylo Voronchenko
- Artem Fliunt
INTRO. What is Git? (in case you missed it)

* Version Control System (VCS)
* Development initiated by Linus Torvalds in 2005
* Essence: keep track and sync file changes
* De facto development standard nowadays
INTRO. What is KSI?

* Keyless Signature Infrastructure
* Scalable digital signature based authentication
* Blockchain - distributed public ledger
* Quantum-proof
* O(t) space complexity
PROJECT. Objective

* Integrate KSI with Git
* Sign commits
* Verify commits
PROJECT. Purpose & Relevance

* Secure development process
* Commits integrity
* Identity check
* Proof of existence
IMPLEMENTATION. Overview

- **git-ksi/**
- **??? git-ksi**
- **??? README.md**

* Python 3
* Single ‘place-everywhere’ script
* Wrapper – can be used instead of Git exec
* Automatically initiates sign/verify process
* Linux tested (should work also on Mac)

https://github.com/arachnid42/git-ksi
IMPLEMENTATION. KSI API

* Guardtime Catena middleware (REST JSON HTTP)
* Precisely: Catena DB with signature persistence:
  - automatically extends signatures to publication
  - assigns rel. short GUIDs to long signatures
  - automatically verifies all signatures in DB
IMPLEMENTATION. Signature Creation

ddnomad@dracula:~/Casino/git-ksi-test$ ls
signme.txt
ddnomad@dracula:~/Casino/git-ksi-test$ git-ksi add .
ddnomad@dracula:~/Casino/git-ksi-test$ git-ksi commit -m 'test commit'
[master 7bb90d6] test commit
  3 files changed, 1 insertion(+), 2 deletions(-)
delete mode 100644 mypie.txt
delete mode 100644 mypresident.txt
create mode 100644 signme.txt
** Please enter your KSI credentials
username: ot.3e3oL5
password:
  >> committed and signed **successfully**! GUID: 7ad440cc-d3ba-47b5-bb3c-3d35d12b9864
IMPLEMENTATION. KSI Verification Policies

* Internal verification (hashing) – implemented by us
* Key-based (PKI) – provided by Catena DB when publication is not available
* Publication-based – provided by Catena DB after publication is out
* Calendar-based – unsupported by Catena
IMPLEMENTATION. Verification

ddnomad@dracula:~/Cinema/git-ksi-test$ ls
ddnomad@dracula:~/Cinema/git-ksi-test$ git-ksi pull origin master
remote: Counting objects: 9, done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 9 (delta 0), reused 9 (delta 0), pack-reused 0
Unpacking objects: 100% (9/9), done.
From github.com:arachnid42/git-ksi-test
  * [new branch]   master   -> origin/master
** Please enter your KSI credentials
username: ot.3e3oL5
password:
** Please enter GUID of the commit you are pulling:
GUID: 7ad440cc-d3ba-47b5-bb3c-3d35d12b9864
>> verification successful! Commit author: ddnomad
<ddnomad@protonmail.com>
From github.com:arachnid42/git-ksi-test
  * branch   master   -> FETCH_HEAD
DEMONSTRATION
PROJECT. Further Plans

* Signing/verifying Git tags
* Securely caching Catena DB access credentials
* Windows support?
PROJECT. Final Thoughts

* Got our hands on production-grade Blockchain technology
* Used API to create something rel. useful
* Got quite a neat overview of Blockchain tech. overall