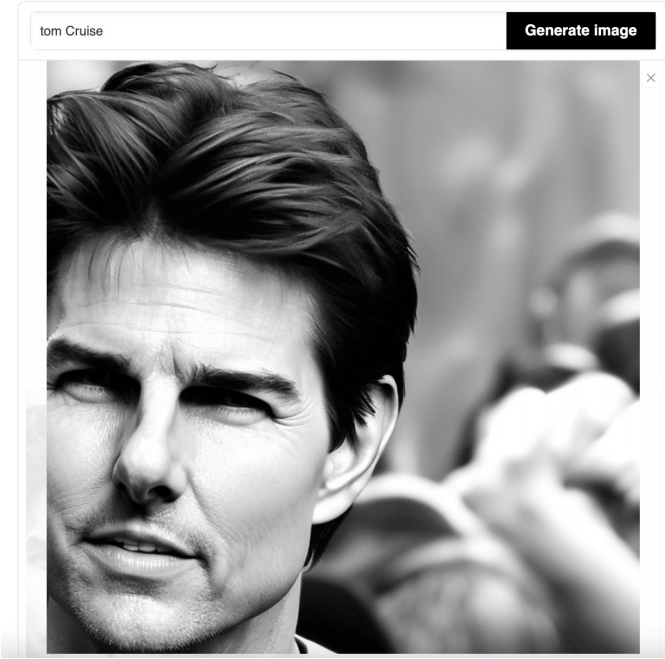
Signet-ring[1,2]: authentic and confidential sharing of digital objects

Amangeet Samra
Amrita Mande
Catherine Jimerson
Diamond Rorie
Mahesh Arumugam

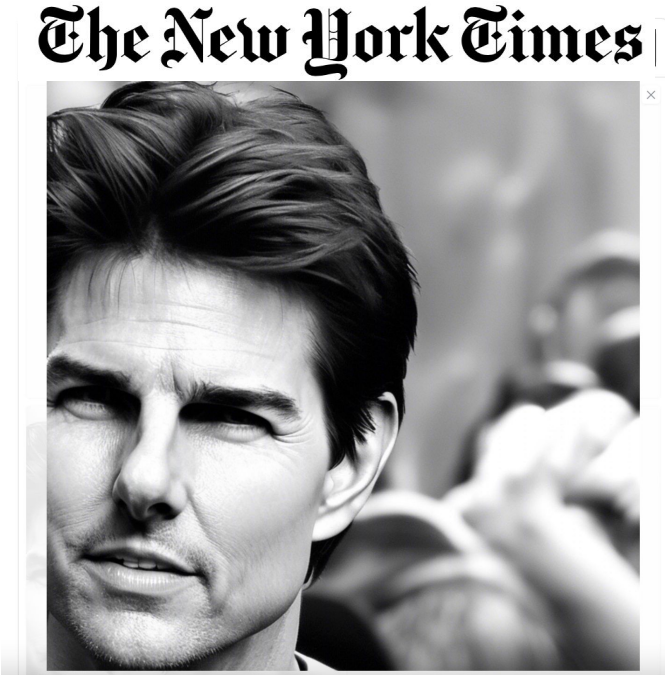
[1] *signet*: “a seal used officially to give personal authority to a document in lieu of signature”
[2] *Signet ring*: “a finger ring engraved with a signet, seal, or monogram”

Motivation



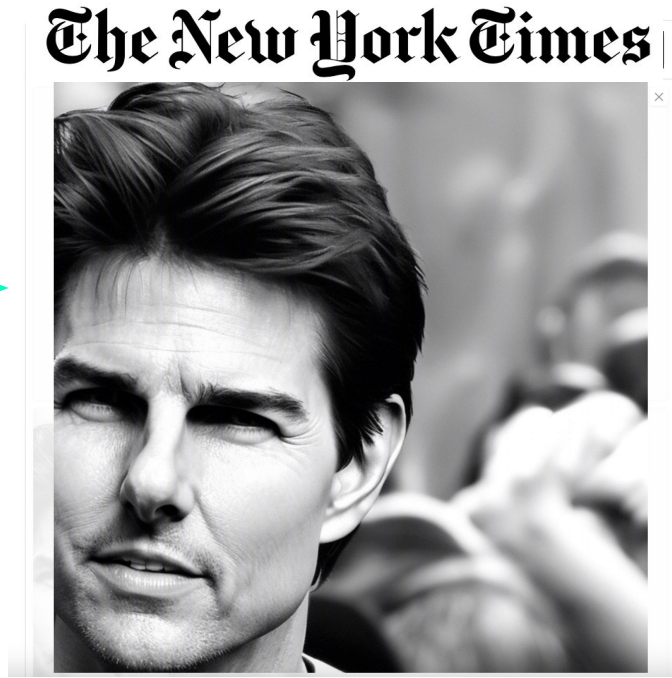
Model by Stability AI - Gradio Demo by 🤗 Hugging Face using the 🧨 diffusers library

Motivation



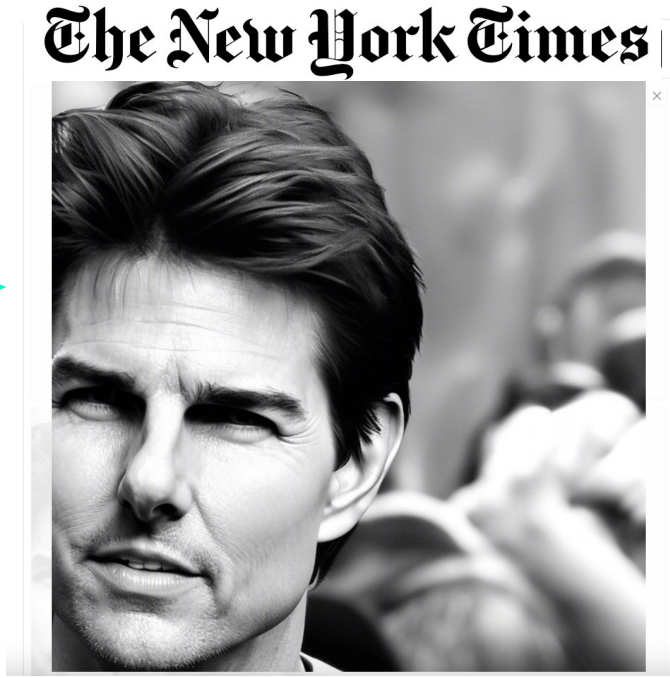
Model by Stability AI - Gradio Demo by 🤗 Hugging Face using the 🧨 diffusers library

Motivation



Model by Stability AI - Gradio Demo by 🤗 Hugging Face using the 🧨 diffusers library

Motivation

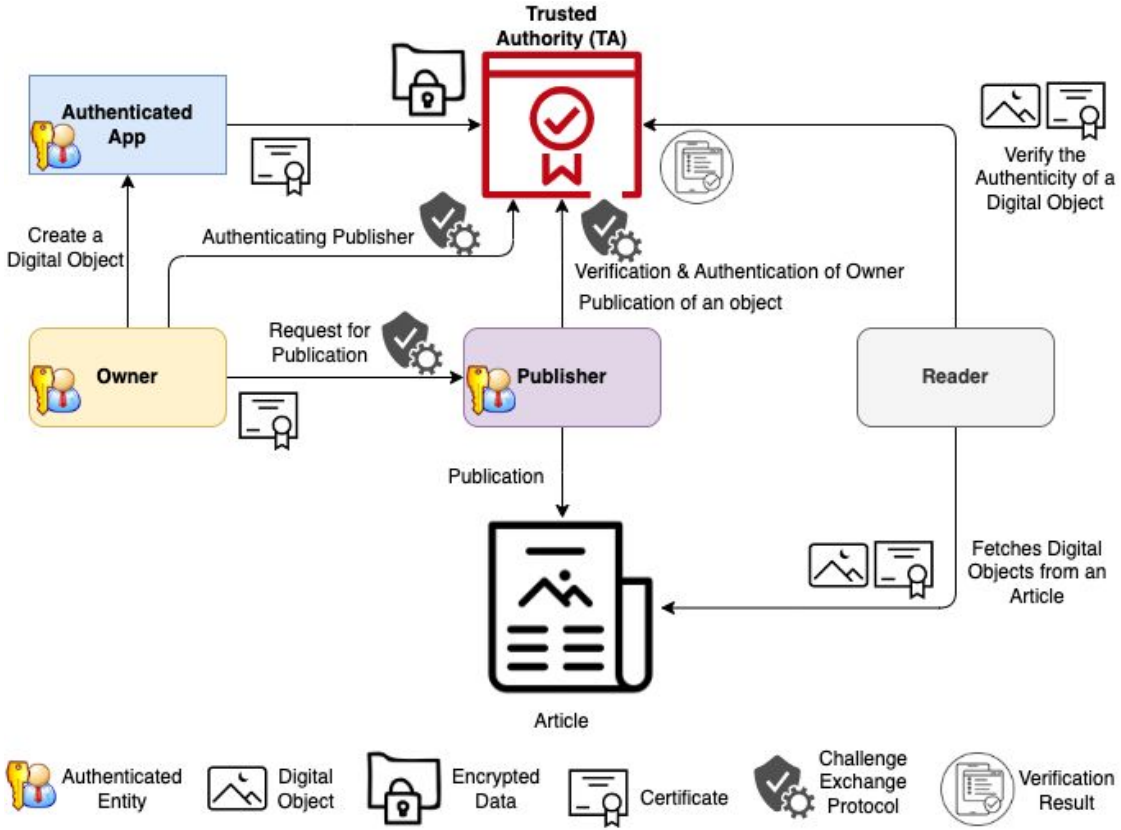


Model by Stability AI - Gradio Demo by 🤗 Hugging Face using the 🧨 diffusers library

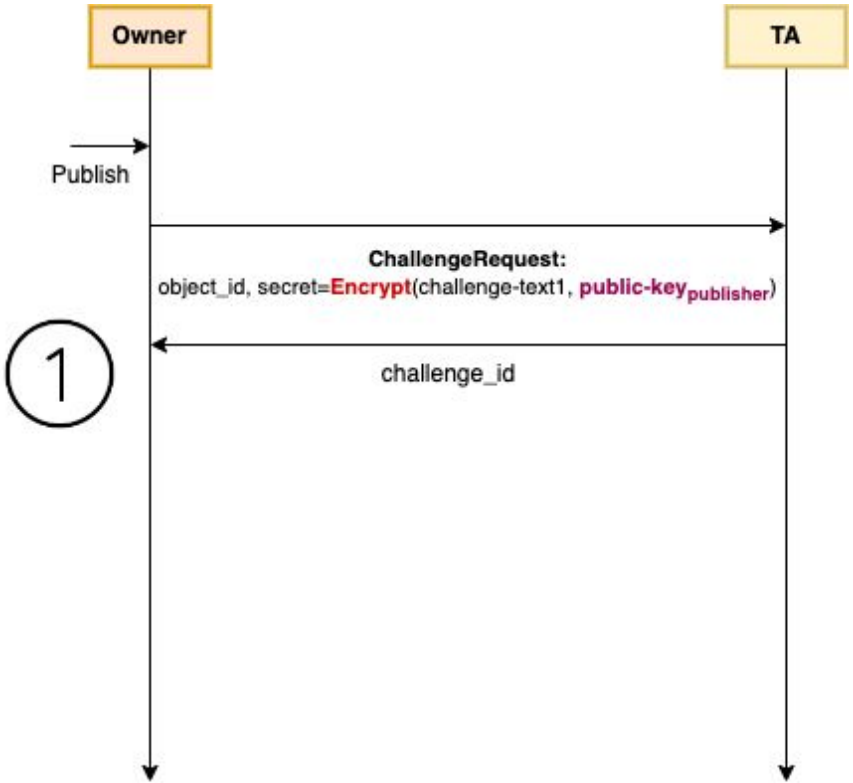
Problem Statement

- Design and implement a system that provides robust authentication services with regard to the sharing of digital objects, (photographs, in news publications)
  - Allows a publisher to authenticate the object through a trusted authority and verify that the source is the owner of the object
  - be able to track any edits made to digital objects to preserve authenticity
- Case for authenticity and confidentiality:
  - Rising spread of fake news, our project aims to ensure the authenticity of a published photograph
  - The changing treatment of socially week information holders by the public

Architecture/API

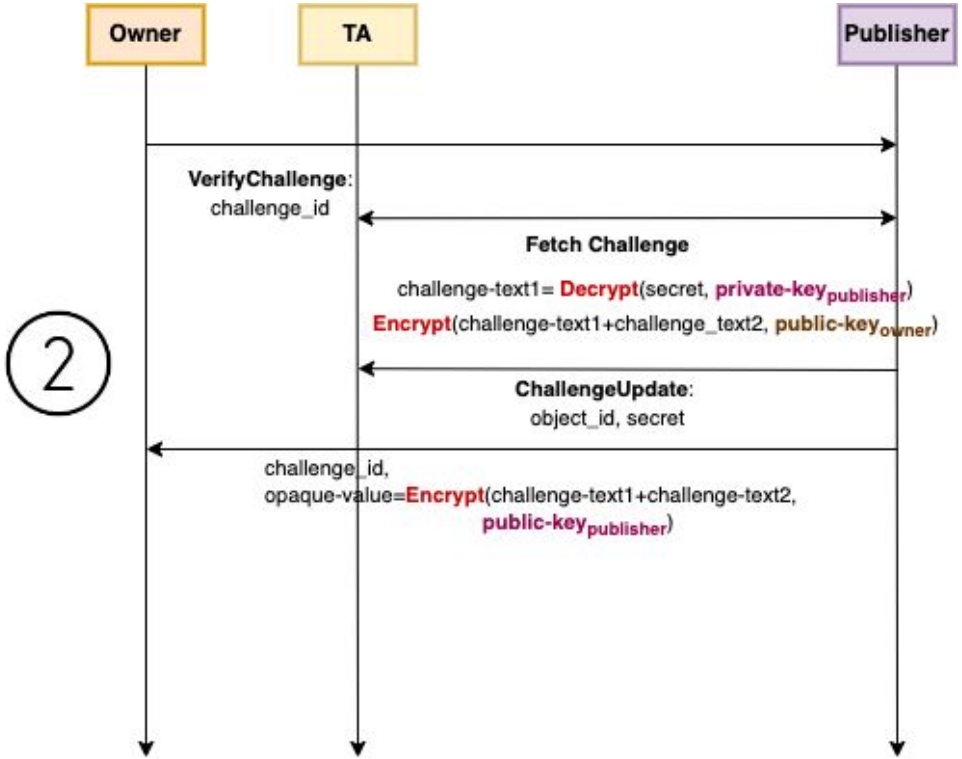


Publication process: Challenge Protocol (1)



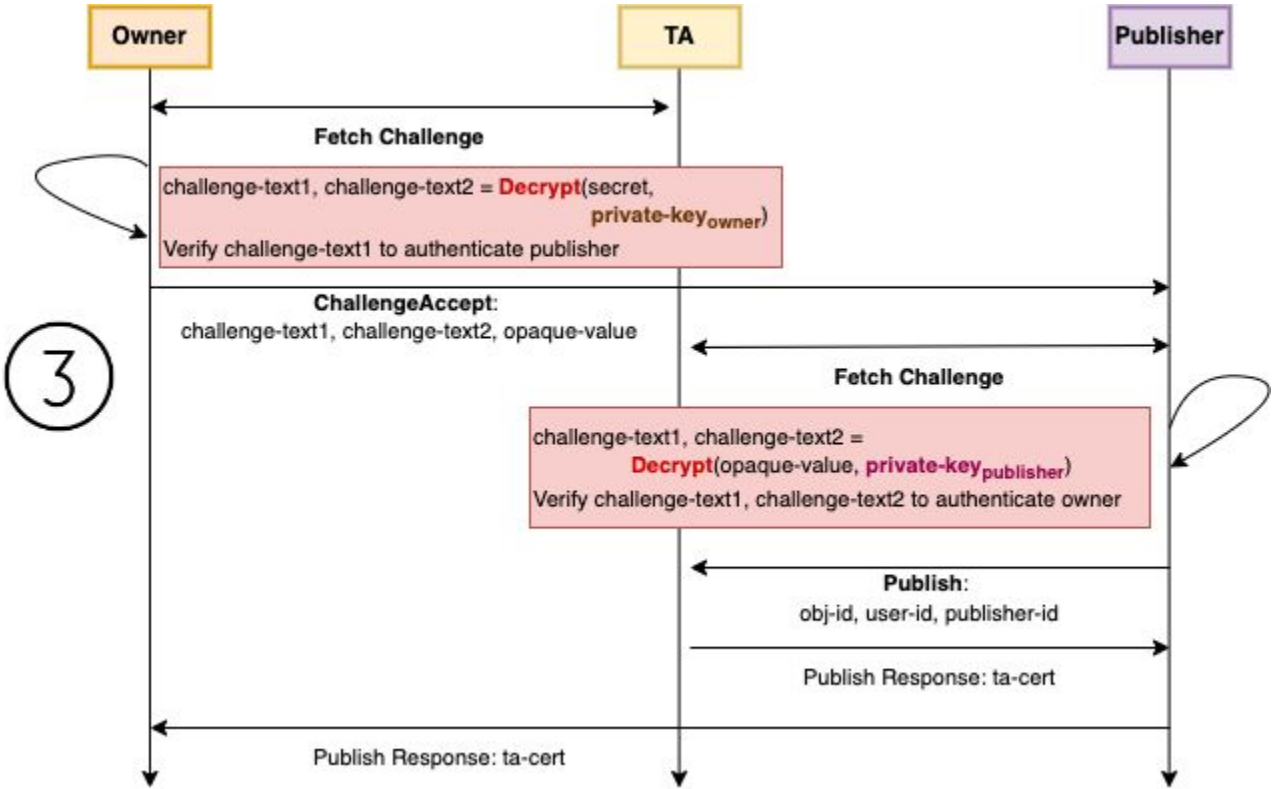
W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

Publication process: Challenge Protocol (2)



W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

Publication process: Challenge Protocol (3)



W. Diffie and M. Hellman, "New directions in cryptography," in *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

Demo: POC Implementation of Signet-ring

3 Python FastAPI servers

- Trusted Authority
- User (instantiated as an Owner or as a Publisher)
- Source App (Camera)

Summary

- Signet-ring addresses
  - The need to track the origin of an image (lineage)
  - The need to try to provide a layer of confidentiality between the owner and the public
- Signet-ring can
  - Certify & authenticate documents
  - Track edits
  - Owners and publishers are able to verify each other

Next Steps

- SSHash[1] check on “similar certified photos”
- Anonymity Everywhere
- Verification of “Real” Users
- Anonymity in Challenge Protocol
- *Verified by Signet-ring*™

[1]Giulio Ermanno Pibiri. Sparse and skew hashing of K-mers. Bioinformatics, Volume 38, Issue Supplement_1, July 2022, Pages i185–i194.

Thank You!

Related Studies

Architecture/API

Is this a real photo?