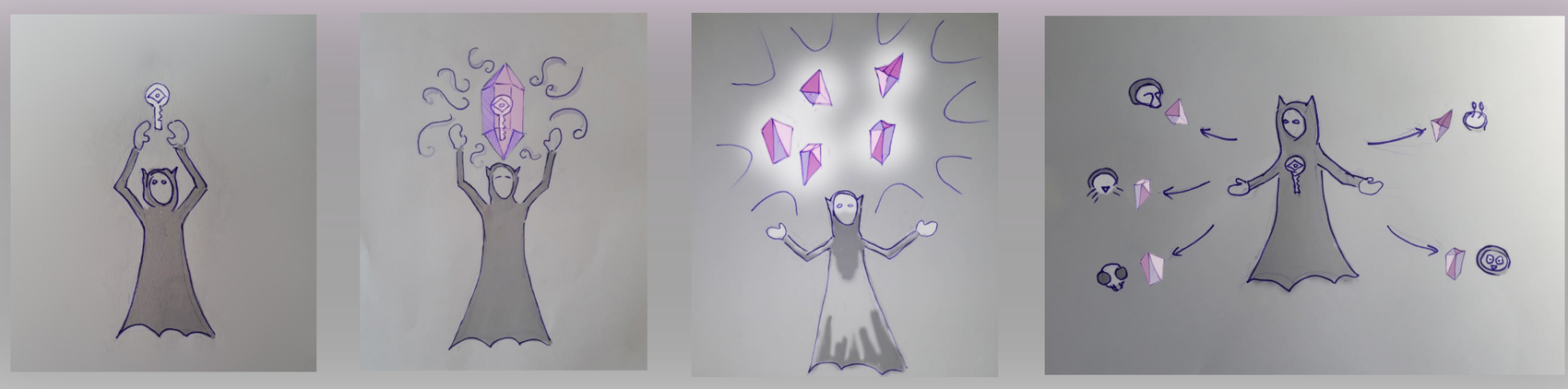
# Dark Crystal

## Verwaltungssystem für Kryptographische Schlüssel

Mit Dark Crystal können Nutzende die Verantwortung für sensible Informationen wie kryptographische Schlüssel unkompliziert über ihre sozialen Netzwerke auf kleine Gruppen von Personen verteilen.

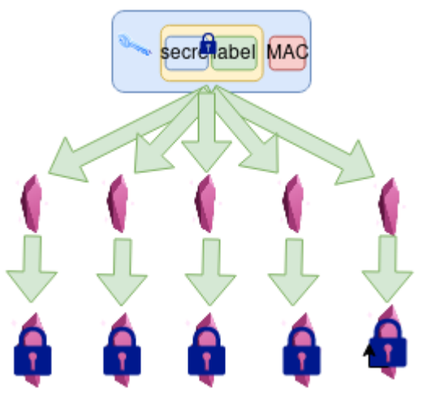


Du teilst deinen Schlüssel auf in 5 'shards'
und schickst sie an deine vertrauten Freunde.

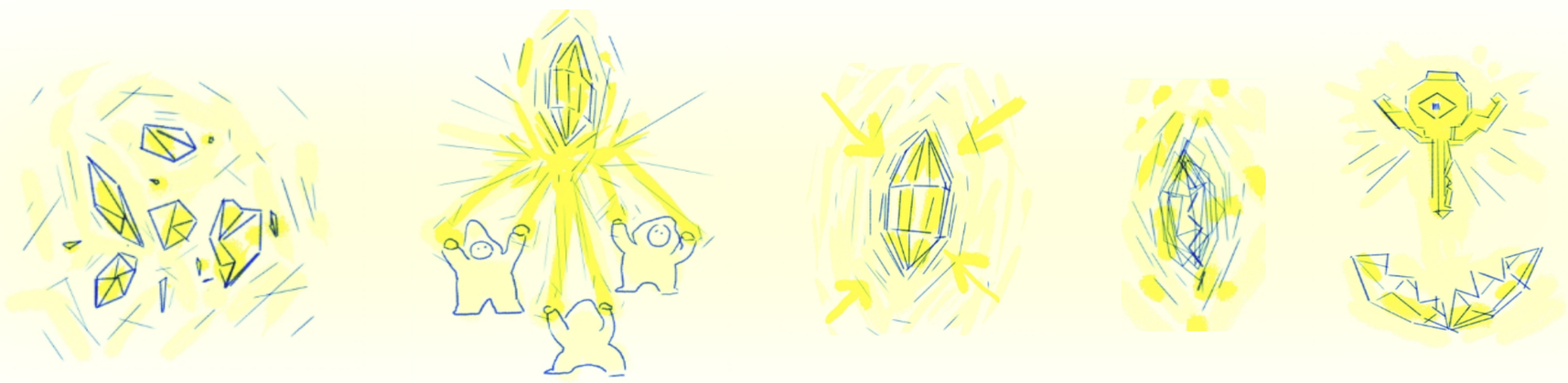

Das Geheimnis wird mit einem beschreibenden Label versehen.


Das Geheimnis wird mit einem symmetrischen Schlüssel verschlüsselt.
Ein Code zur Authentifizierung wird ergänzt.


Auf der Basis eines sicheren, schwellenwertbasierten secret sharing Algorithmus werden 'Shards' generiert




Jedes 'Shard' wird signiert und für jeden vertrauten Kontakt verschlüsselt.



Wenn du dein Gerät verlierst, kannst Du drei deiner vertrauten Freunde fragen, die Shards an deinen neuen Account zu schicken.

Die shards werden entschluesselt und verifiziert.


Die shards werden wieder zu dem Geheimnis zusammengefuegt.


Das Geheimnis wird mit dem MAC verifiziert

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Prototype Fund



https://dark-crystal.gitlab.io