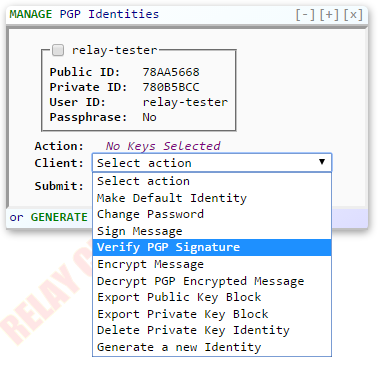
What is Relay Keyspace

(ask a question and it will be answered)

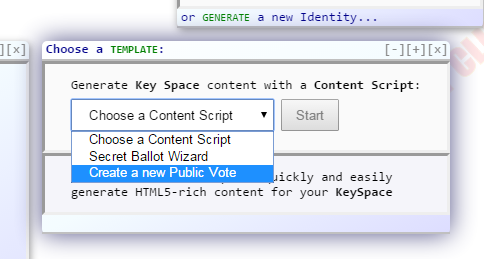
WHAT IS RELAY KEYSPACE?

While using Relay, users manage their public identities with **PGP Key Pairs**. With each Key Pair created, owners of that pair may publish **KeySpace Content** into the KeySpace belonging to that Identity. In other words, any content (text, HTML, images) you sign with your **PGP Private Key** belongs to the **KeySpace** associated with that Private Key. This works because only you can create signatures with your PGP Private Key. Everyone on the Relay network knows it’s *your content* because they can verify your **pgp signature** using your **PGP Public Key**. The Relay Client and Server perform this verification automatically as KeySpace content is consumed and relayed across the network.

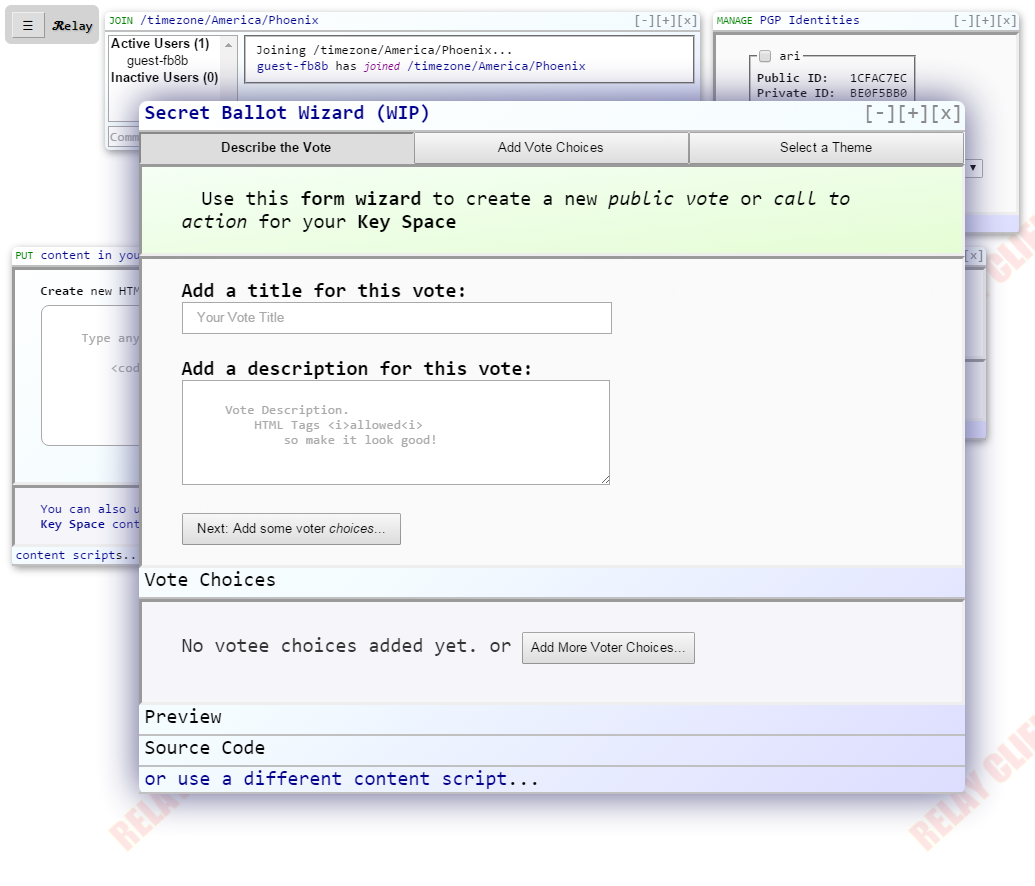


# ALL RELAY CONTENT IS ENTERED INTO A ‘KEYSPACE’

Relayers may type in content directly or use one of the available Content Wizards to generate and publish content automatically. Relay also facilitates various software functionality. One common example would be Public Votes and Secret Ballots.

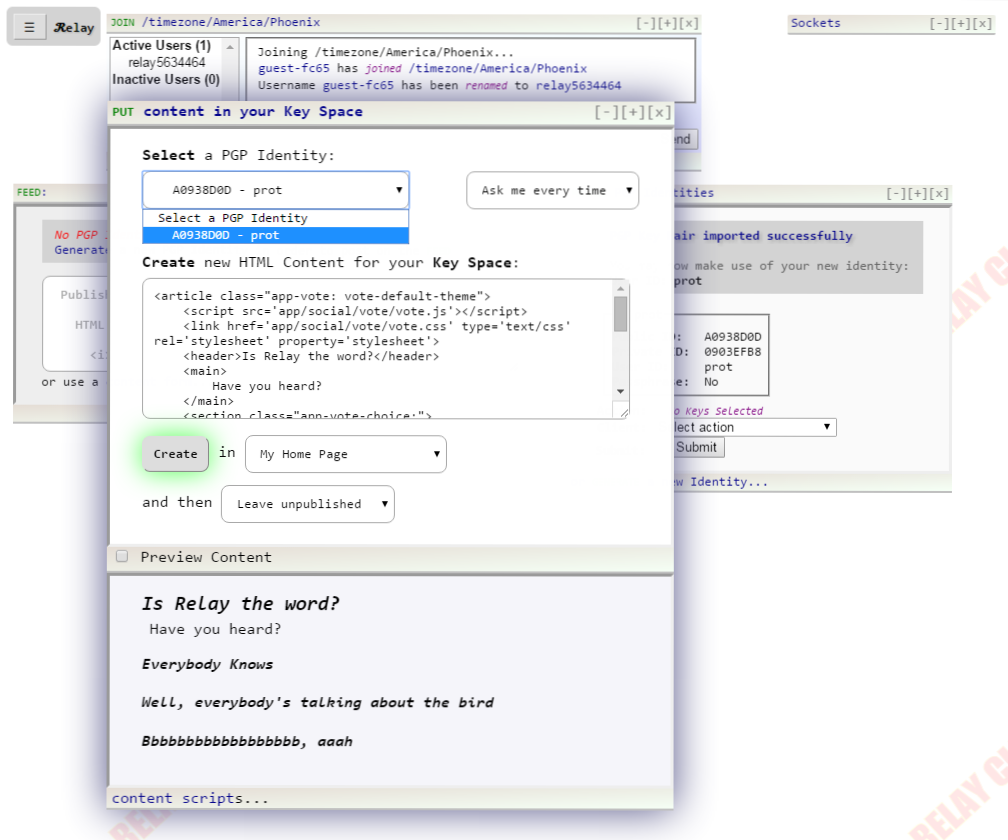


*Creating a secret ballot via a Content Script form wizard:*



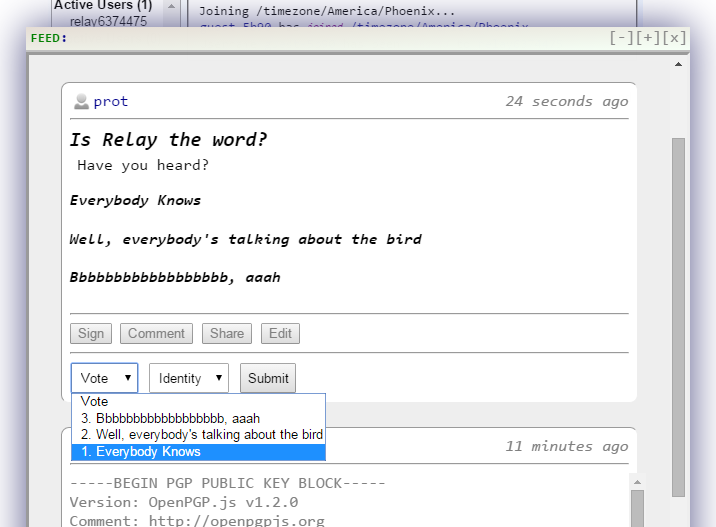
# 

# ALL RELAY CONTENT IS SIGNED BY ITS CREATOR

The chosen PGP Key is used to sign the content before it is published to the network. Other clients can automatically verify the signature as they consume the content.

# RELAYERS ‘ENTER THE KEYSPACE’ TO VIEW SIGNED CONTENT

Relayers access KeySpace Content contributed by other Relayers by authorizing a new Public Key Identity to their own contact list. This is known as ‘entering the keyspace’. KeySpace content is only ever consumed after first being verified locally by the client. Unverified content is ignored both by the client and servers in the Relay Network. The end user sees the new public vote and is able to submit vote entries back to the network via their own KeySpace.



# KEYSPACE CONTENT IS STORED LOCALLY ON THE CLIENT’S BROWSER

KeySpace entries are organized by PGP Key ID and Timestamp, and typically include a *path*. Public Key Blocks are stored at “public/id” while Private Key Blocks are stored at “.private/id”. The period prefix indicates that content in the “.private/” folder should never be sent to the network. Other content may be created in the user’s home directory, or a directory corresponding with another user or service.

View of IndexedDB entries in a Client Browser

