Blockchain Commons

Advocating for the Creation of Open, Interoperable, Secure, and Compassionate Digital Infrastructure

Envelope Request & Response

What is Request & Response?

- Envelope functionality
- Allows one device to request something from another
    - Interoperability
    - Automation
- See our new Implementation Guide
    - BCR 2024-04
    - https://tinyurl.com/bcr-2024-004

TL;DR? They're Expressions

- Requests are build on Expressions
    - A FUNCTION
    - With 0 or more PARAMETERS
    - Each of which has an ARGUMENT

```
«getSeed» [
        ❮seedDigest❯: Digest(ffa11a8b)
]
```

Expressions with Results

- Results simply return the requested object
    - with an `isA` to provide definition
    - and maybe other metadata

```
Bytes(16) [
        'isA': 'Seed'
        'hasName': "Dark Purple Peck Vial"
        'outputDescriptor': output-descriptor(Map)
]
```

Wrapping It Up

- That Expression and the result are wrapped as Request/Response
    - And marked with an ARID (random ID)
- Request Has Expression as a `body`
    - Maybe other metadata like a `note`!

```
request(ARID(7b33b86e)) [
    'body': «getSeed» [
        ❰seedDigest❱: Digest(ffa11a8b)
    ]
    'note': "Alias quam ullam qui reprehenderit ad quibusdam in hic occaecati aut ut vol
]
```

The Response

- Response similarly has result as a `response`
  - Using the same ARID

```
response(ARID(7b33b86e)) [
    'result': Bytes(16) [
        'isA': 'Seed'
        'hasName': "Dark Purple Peck Vial"
        'outputDescriptor': output-descriptor(Map)
    ]
]
```

There Are Details

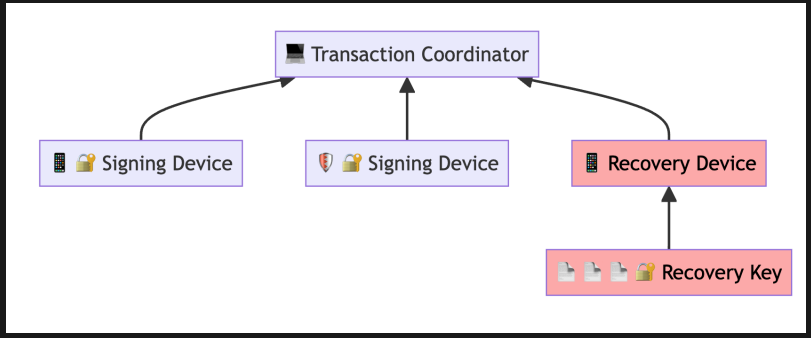
- Requests and Responses are coded with CBOR tags
- `function` and `parameter` are defined with values
- Everything Uses Known Values
- It's All in the Implementation Guide!
    - https://tinyurl.com/bcr-2024-004

So WHY use
Request/Response?

Obviously, they're an interoperable way to communicate.

But we think they're
even more important
to automate complex tasks.

Automating Tasks with Request/Response



- Multisigs are our current best use case
  - We *want* people to use multisigs
  - We wrote a whole scenario to do so
    - https://tinyurl.com/multisigs
  - But it's complex to create a multisig!

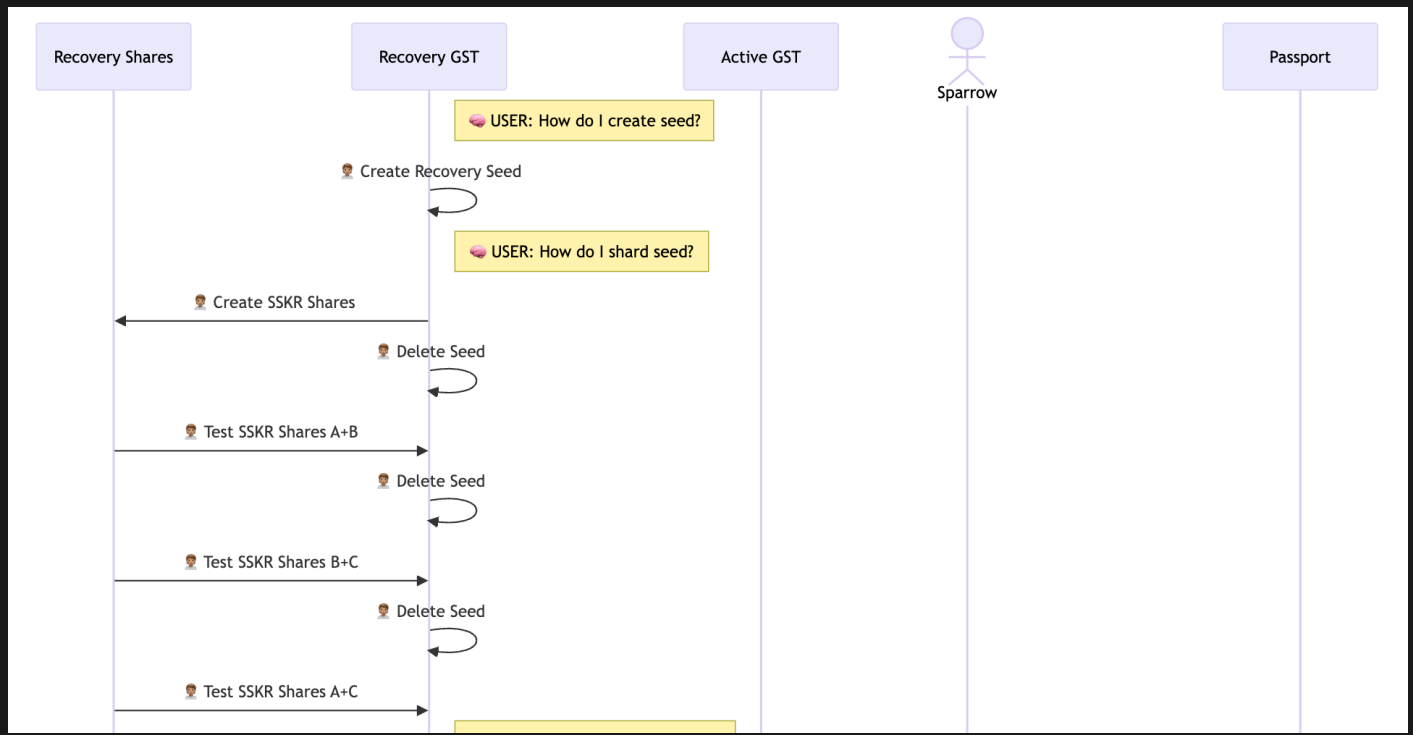
Three Complexities in Non-Automated Systems

1. Decision Points
    - User decides what to do
2. Research Points
    - User figures out how things work
3. Human Actions
    - User pushes buttons

The more decision points, research points, and human actions, the less likely that a user actually finishes a task, and there can be a LOT in a complex interaction.

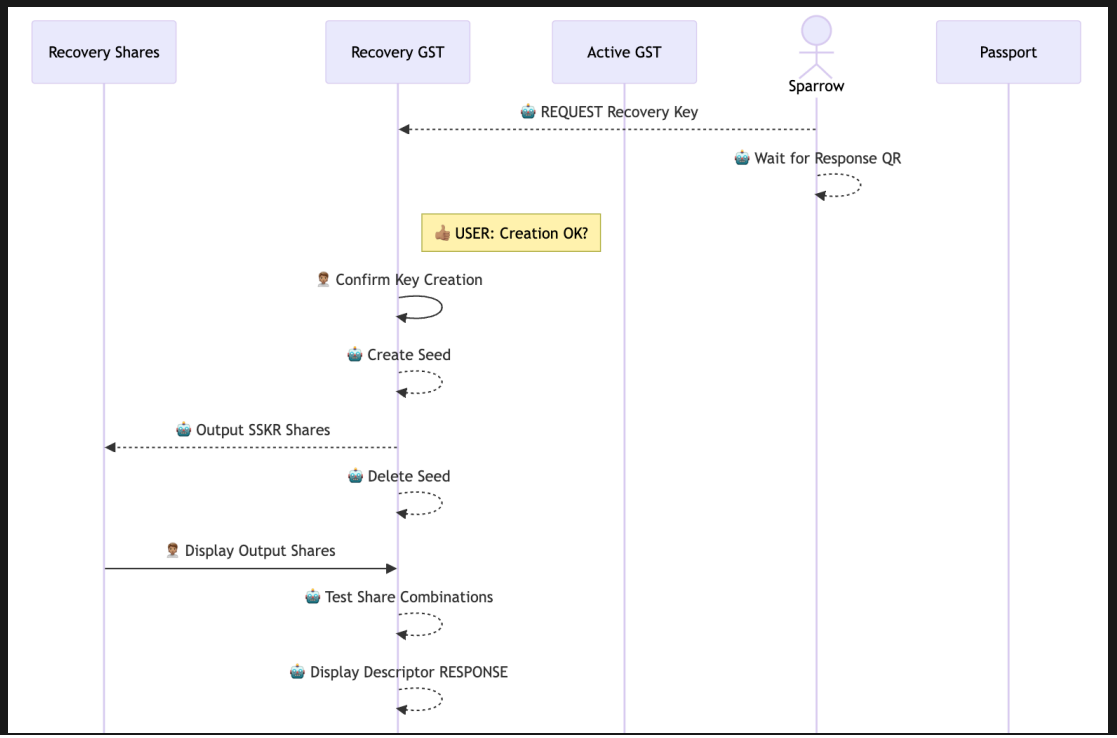
The State of the Art for Multisig

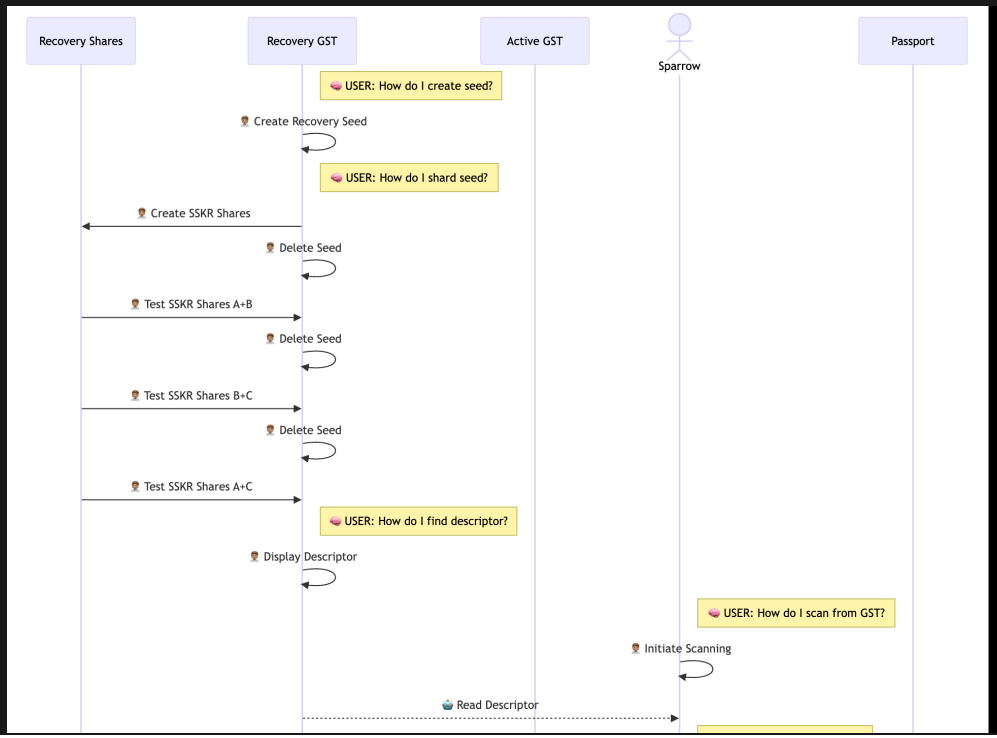
- Right now a user has to KNOW a procedure
- He has to KNOW what to do on each device to create a multisig
- He must be a very knowledgeable CONDUCTOR

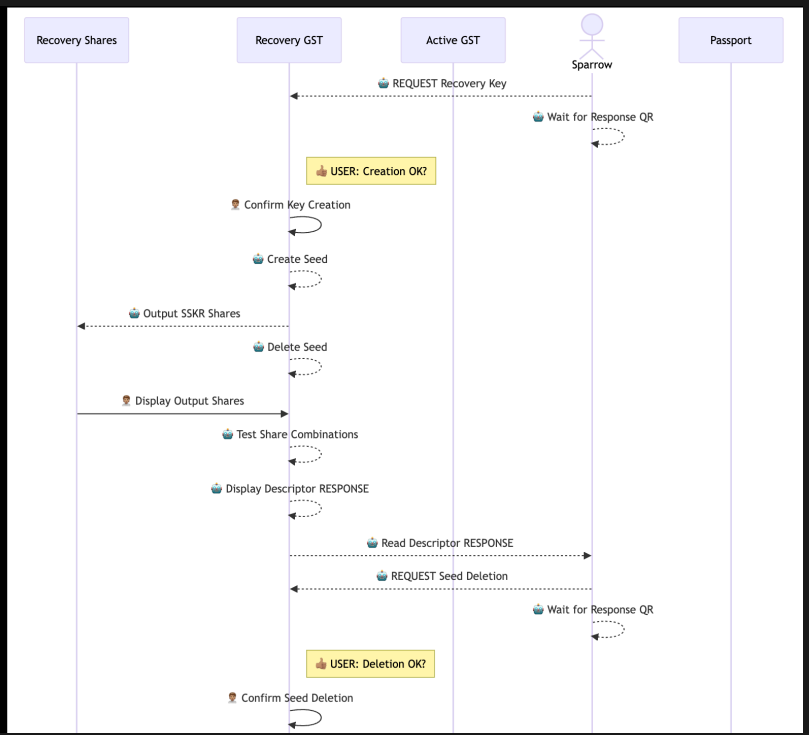

Recovery Shares
Recovery GST
Active GST
Sparrow
Passport
USER: How do I create seed?
Create Recovery Seed
USER: How do I shard seed?
Create SSKR Shares
Delete Seed
Test SSKR Shares A+B
Delete Seed
Test SSKR Shares B+C
Delete Seed
Test SSKR Shares A+C

Response/Request for Multisig

- Lets a Network Coordinator Be the CONDUCTOR
- It Makes Decisions CENTRALIZED
- It Tells The User What to Do
- It Communicates with Devices
    - Rather than the User Jumping Around on their Own
- It Tells the Devices What to Do
    - Rather the the User Having to Know HOW
- The User CONFIRMS
- The User take PHYSICAL ACTIONS


Recovery Shares
Recovery GST
Active GST
Sparrow
Passport
REQUEST Recovery Key
Wait for Response QR
USER: Creation OK?
Confirm Key Creation
Create Seed
Output SSKR Shares
Delete Seed
Display Output Shares
Test Share Combinations
Display Descriptor RESPONSE


Recovery Shares
Recovery GST
Active GST
Sparrow
Passport
USER: How do I create seed?
Create Recovery Seed
USER: How do I shard seed?
Create SSKR Shares
Delete Seed
Test SSKR Shares A+B
Delete Seed
Test SSKR Shares B+C
Delete Seed
Test SSKR Shares A+C
USER: How do I find descriptor?
Display Descriptor
USER: How do I scan from GST?
Initiate Scanning
Read Descriptor


Recovery Shares
Recovery GST
Active GST
Sparrow
Passport
REQUEST Recovery Key
Wait for Response QR
USER: Creation OK?
Confirm Key Creation
Create Seed
Output SSKR Shares
Delete Seed
Display Output Shares
Test Share Combinations
Display Descriptor RESPONSE
Read Descriptor RESPONSE
REQUEST Seed Deletion
Wait for Response QR
USER: Deletion OK?
Confirm Seed Deletion

What Does Request/Response Give Us?

	Classic	R/R
Decision Points (💡)	5	2
Confirmation Points (👍🏾)	0	6
Research Points (🧠)	11	1
Human Actions (🧑🏽‍💻)	31	14
Automated Actions (🤖)	5	33

For More On Request/Response

- Take a look at our full use case:
  - In our Smart Custody Repo
  - https://tinyurl.com/multisigs-rr
- Implement with the implementation guide:
  - In our Research Repo
  - https://tinyurl.com/multisigs

www.BlockchainCommons.com

Shannon Appelcline (@shannona)