

Federated, not out of control

How SBGs and CDGs keep federation under control
20.09.2024

Patrick Maier // @pmaier:element.io

Agenda

1. The challenge
2. Technology and scaling
3. Use cases & customer applications
4. Vision, outlook & summary

1. The challenge

Decentralization is key to Matrix' success element

[m]

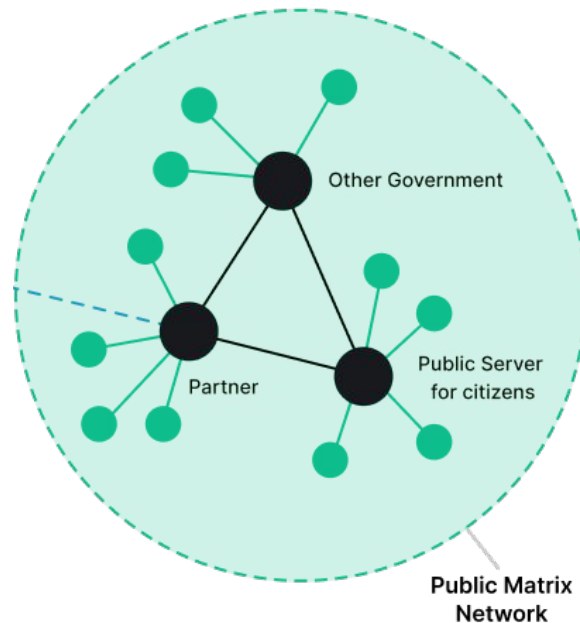
Open

Decentralized

Federated

Privacy-preserving

Choice



... but it comes with threats and risks

Uncontrolled
data replication

Compliance?

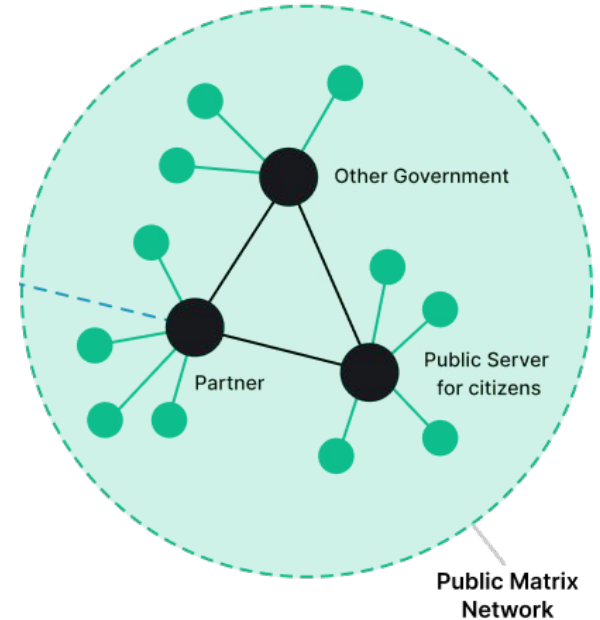
Data loss
risks

Communication
rules?

Espionage

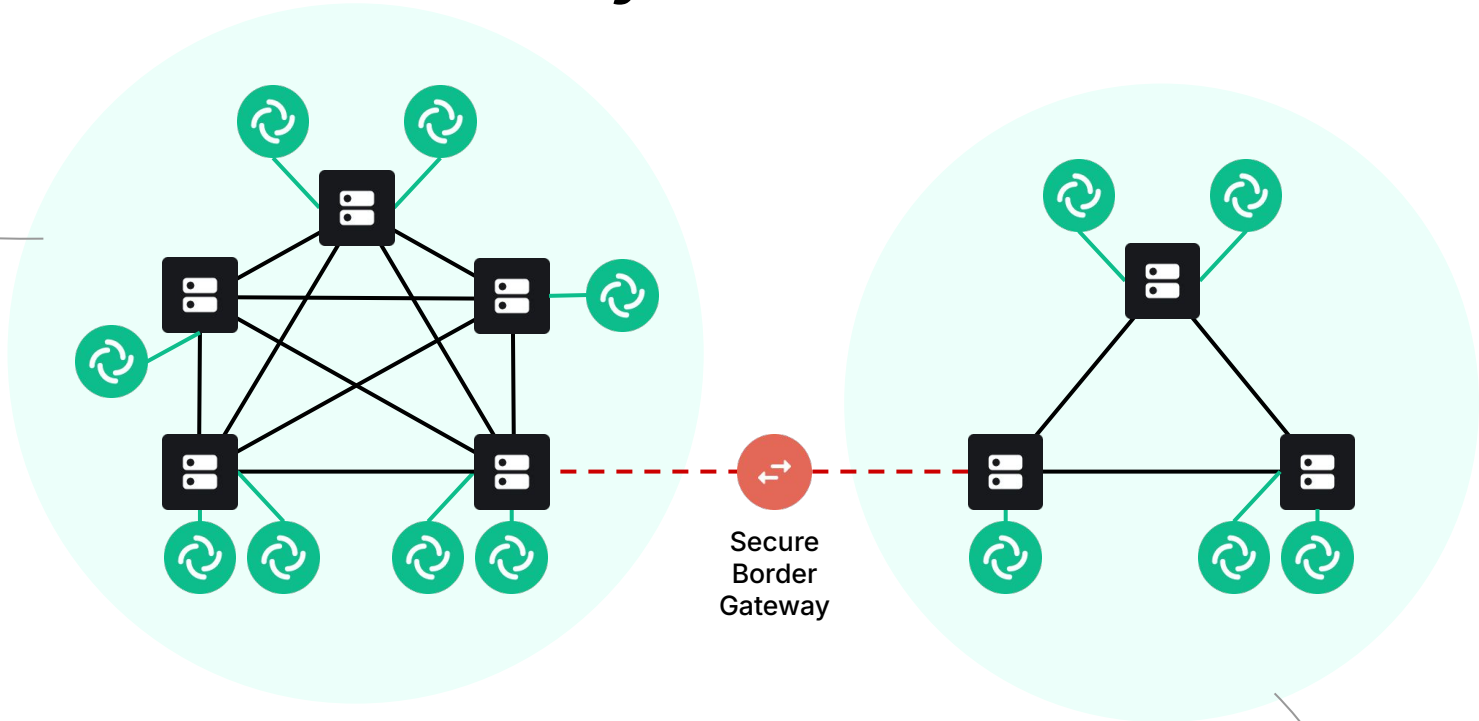


Insecure
homeservers



Secure Border Gateway - The solution

Governmental
Matrix network



Secure
Border
Gateway

Public Matrix network

So, instead of taking threats and risks...

Uncontrolled
data replication

Compliance?

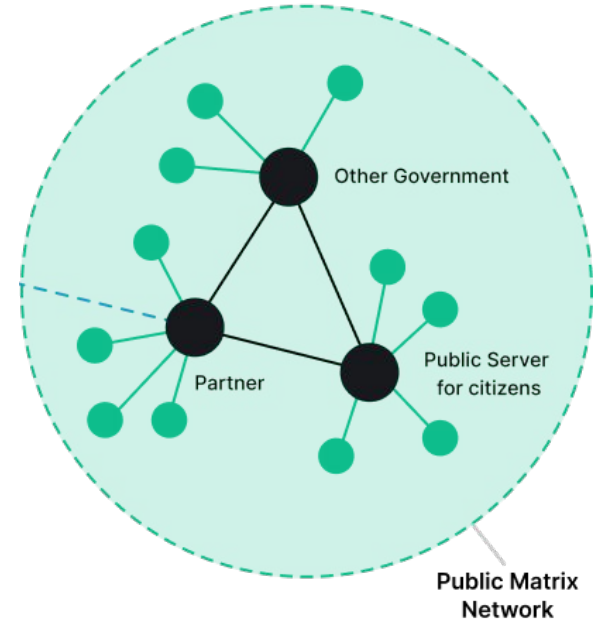
Data loss
risks

Communication
rules?

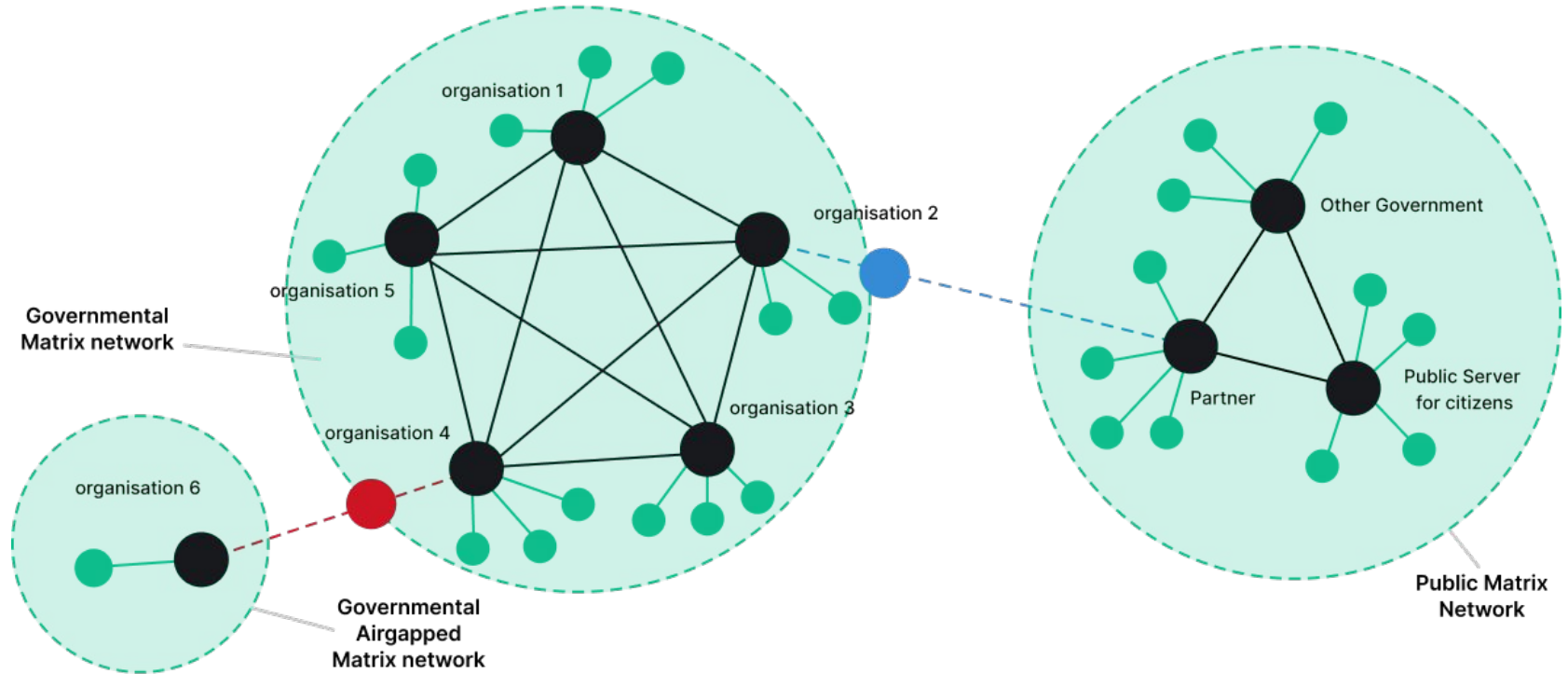
Espionage



Insecure
homeservers



...we control federation with SBGs/CDGs

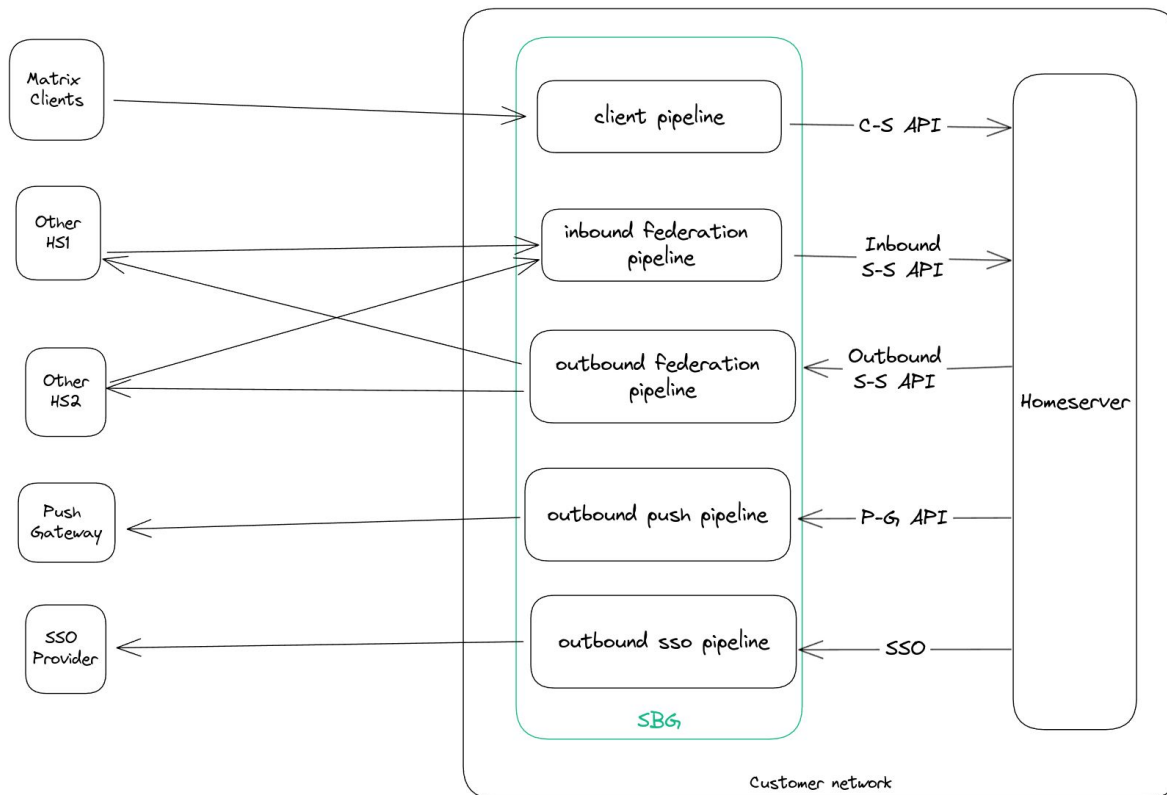


2. Technology & scaling

Secure Border Gateway - Overview

- **Application-level firewall** for Matrix homeservers
- Inspects **all requests** to and from the homeserver
- Can use all request **metadata** to enforce rules
- **Pipeline**-based approach to connect APIs and rule sets
- Pluggable **rules engine** that can be applied to the pipelines
- Flexibility: Additional rules engines can be developed as **SBG modules**
- **Available to Element customers (shipped & integrated with ESS)**

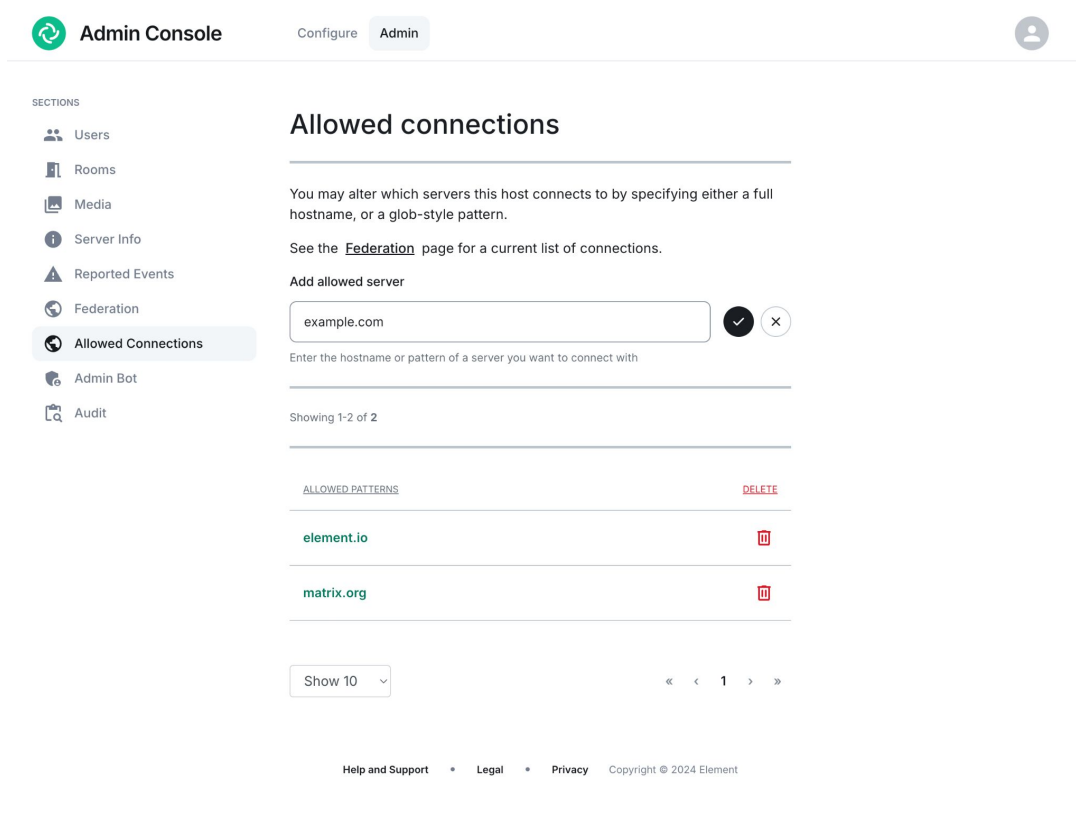
SBG fully shields homeservers




SBG is made to scale

- Based on modern technologies (Rust) to make it high-performance, robust and resilient
- Low resource footprint
- Stateless & cloud-native
- Horizontal scaling for availability and load distribution

SBG integrates with the ESS admin console element



Admin Console Configure Admin 

SECTIONS



- Users
- Rooms
- Media
- Server Info
- Reported Events
- Federation
- Allowed Connections**
- Admin Bot
- Audit

Allowed connections

You may alter which servers this host connects to by specifying either a full hostname, or a glob-style pattern.



See the [Federation](#) page for a current list of connections.


Add allowed server

Enter the hostname or pattern of a server you want to connect with

Showing 1-2 of 2

ALLOWED PATTERNS	DELETE
element.io	
matrix.org	

Show 10 

« < 1 > »

[Help and Support](#) • [Legal](#) • [Privacy](#) Copyright © 2024 Element

SBG - Current capabilities

- Private Federation Enforcement
 - Block traffic to/from certain domains completely (deny list)
 - Allow traffic only to/from certain domains (allow list)
- Gematik TI-Messenger: Messenger proxy
 - Use an externally managed federation list
 - Enforce rules on room invites (3-step permission concept)
 - User-driven *Contact Management*
 - *Rohdatenerfassung* (performance and inventory data capture)
- Modularity and generic approach allows you to do anything
 - Any metadata on the pipelines can be used to allow/deny requests
 - Request metadata can be rewritten

Special Case: Cross Domain Gateways

- Enables national security level communication
 - Separate networks of different classification levels (low side vs. high side) and span airgaps
 - Allow controlled communication between the networks
 - Full transparency on all traffic (metadata & content)
 - Ability to interfere on all traffic
- CDG today
 - Blueprint and toolbox for building Cross Domain Gateways
 - Pure software or running on COTS or bespoke hardware
 - A benign machine-in-the-middle (MITM) that will decrypt and re-encrypt content
 - Can find and replace terms in message contents that shouldn't leave the high side

3. Use cases & customer applications


The messenger for German healthcare



TI-M Pro




TI-M ePA



element
by the creators of Matrix

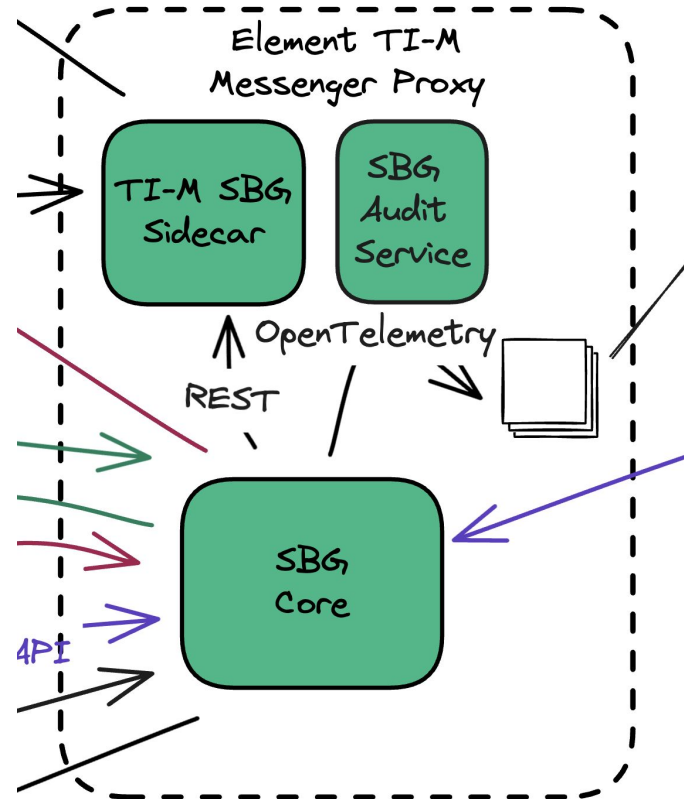
A backend for TI-Messenger.

A Matrix-based server that's ready for Gematik's TI-Messenger Fachdienst

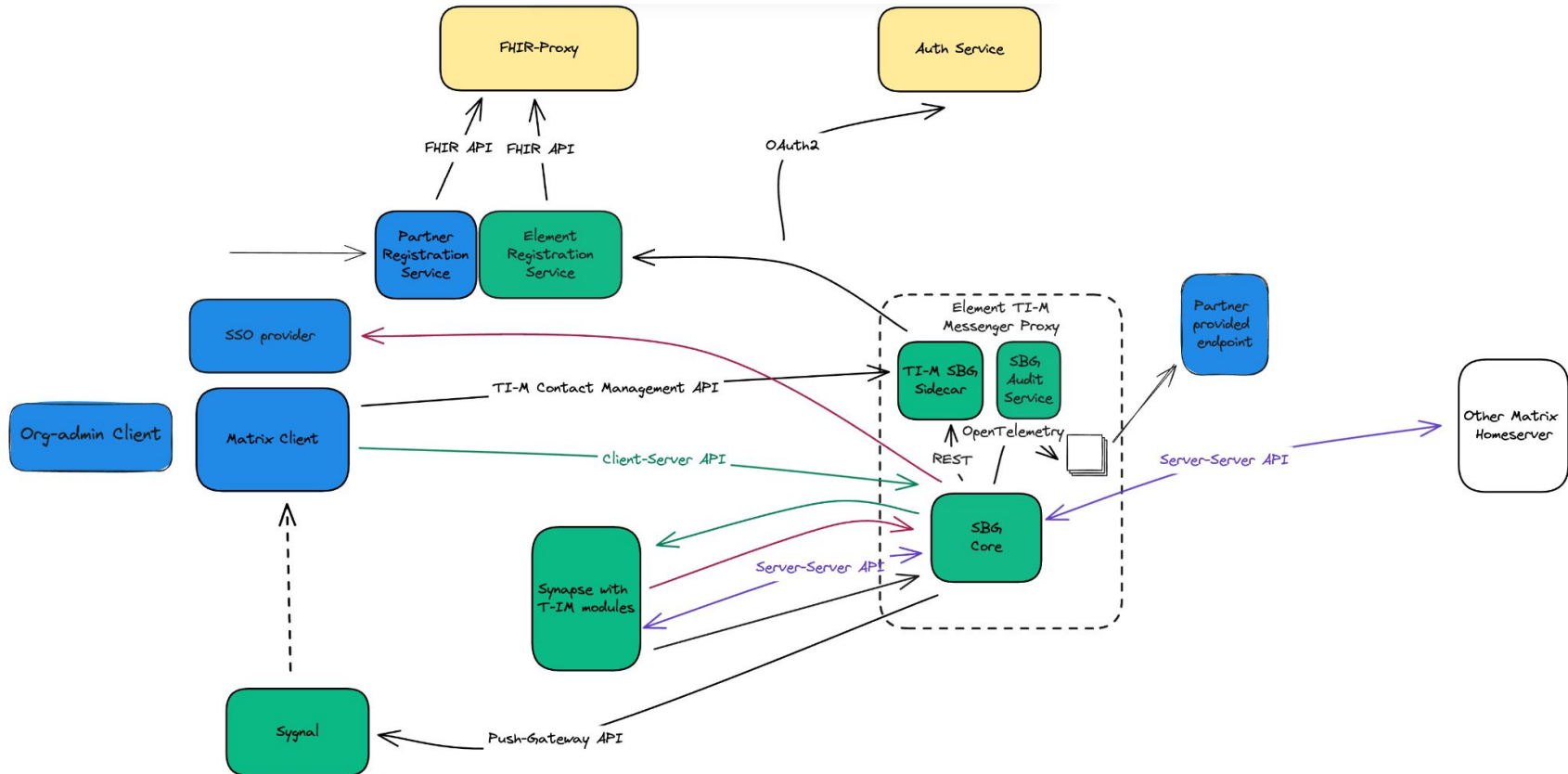
A diagram showing two overlapping blue rounded squares. The top square contains a white icon of two USB drives. The bottom square contains a white icon of a smartphone with a green outline and two white arrows pointing in opposite directions.

Elevating communication
in healthcare across Germany

At the heart of Gematik TI-Messenger



At the heart of Gematik TI-Messenger



4. Vision & outlook

Vision and outlook

- Every professional Matrix server should deploy an SBG alongside to keep users safe and and ensure compliance
- ESS makes this a breeze for Element customers
- Same for CDG in the right use cases ⇒ Element will support you in making required customizations

- The products' feature-sets will grow to solve even more challenges
 - TI-Messenger 2.0/ePA support
 - Policy enforcement for room memberships on a user- and group-basis
 - Using LDAP/AD attributes to control the policies
 - Information governance with security labels (XEP-258 compatible)
 - <Your favorite usage example>

Summary

- SBG (and CDG) are your **compliance tools** for Matrix servers
 - SBG is an application-level firewall that relies on request metadata
 - CDG is a benign MITM to inspect and modify message contents
- Both are **in active use with customers** today and have proven to solve real-world challenges
- Their generic and modular approach allows to flexibly **adapt to individual needs**

Questions?