

# Implementing Security Labels in Matrix.

# Who we are.



**Midhun Suresh R**

Software Engineer • Element  
[@rmidhunsuresh:matrix.org](mailto:@rmidhunsuresh:matrix.org)



**Kieran Lane**

Technical Engineer • Element  
[@kieranml:element.io](mailto:@kieranml:element.io)

# The Problem.

In defence and government simply being in the room isn't enough to secure messaging.

- Every message needs its own security label, checked against each reader's clearance.
- Mainstream chat labels the room at most, and every message inherits it.
- Organisations that need per-message labels end up stuck on XMPP.

## Standard chat

Name the room, maybe adding "Secret"

## Labelled Chat

Maximum label of room; labels per message

TOP SECRET

OFFICIAL

SECRET

TOP SECRET

REL TO CAN

REL TO NATO

INT

# Why Matrix.



## End-to-End Encrypted

Messages are encrypted on the device, so servers relay them without being able to read them.



## Tamper-evident history

Every message is fingerprinted and linked to the ones before it, so history can't be rewritten unnoticed.



## Federation and Sovereignty

Each nation runs its own servers and keeps its own data, while sharing rooms with the others.



## Extensible

Messages are structured JSON that can carry extra fields, like a security label, without breaking existing clients.

# Security Labels.

TOP SECRET

REL TO NATO

INTELLIGENCE

SECURITY

CONFIDENTIAL

REL TO FVEY

MANAGEMENT

SECRET

REL TO CAN

RED

APPOINTMENTS

SANS CLASSIFICATION

REL TO AUS

ERITTÄIN SALAINEN

SIOP

LEGAL

CONFIDENTIEL

OPERATIONS

UNMARKED

CRYPTO

DIFFUSION RESTREINTE

COMMERCIAL

PUBLIC

REL TO NZL

OFFICIAL

BAR

KÄYTTÖ RAJOITETTU

FOO

MEDICAL

REL TO USA

UNCLASSIFIED

ATOMAL

FINANCE

BUDGET

RESTRICTED

BLUE

INTERNAL

REL TO DEU

SIOP ESI

SALAINEN

EXCLUSIVE

LOGISTICS

TRÈS SECRET

REL TO FRA

OFFICIAL-SENSITIVE

STAFF

BOHEMIA

PERSONAL

# NATO Standards.

## RULEBOOK

**What labels are allowed?**

SPIF: XML SPIF 2.1 + NATO extensions  
ADatP-4774 · 4774.1 · 4774.5

## LABEL

**What does one label look like?**

CMLS confidentiality label, as XML or JSON  
ADatP-4774.5 (XML) · ADatP-4774.7 (JSON)

## BINDING

**How is a label attached to data?**

A binding, profiled per protocol: email, XMPP, Office...  
ADatP-4778 · 4778.2 · 4778.7 (JSON)

**Using these standards and definitions** the MSC can define where and how a label lives in Matrix.

Policy

Label

Syntax

Room

Event

Client

Server

# Security Policy Syntax.

A Security Policy Information File defines every label a policy allows.

- Classifications, ranked to denote hierarchy
- Category tags, each permissive, restrictive or informative
- How each value renders as a marking, i.e. colour, multi-selection, excluded classes etc.

GBR

SECRET

REL TO FVEY

INT

BUDGET

```
<securityPolicyId name="GBR">
  <securityClassification name="OFFICIAL" lacv="3"/>
  <securityClassification name="SECRET" lacv="4"/>
  <securityClassification name="TOP SECRET" lacv="5"/>

  <securityCategoryTag enumType="permissive"
    name="Releasable To">
    <tagCategory name="FVEY"/>
  </securityCategoryTag>

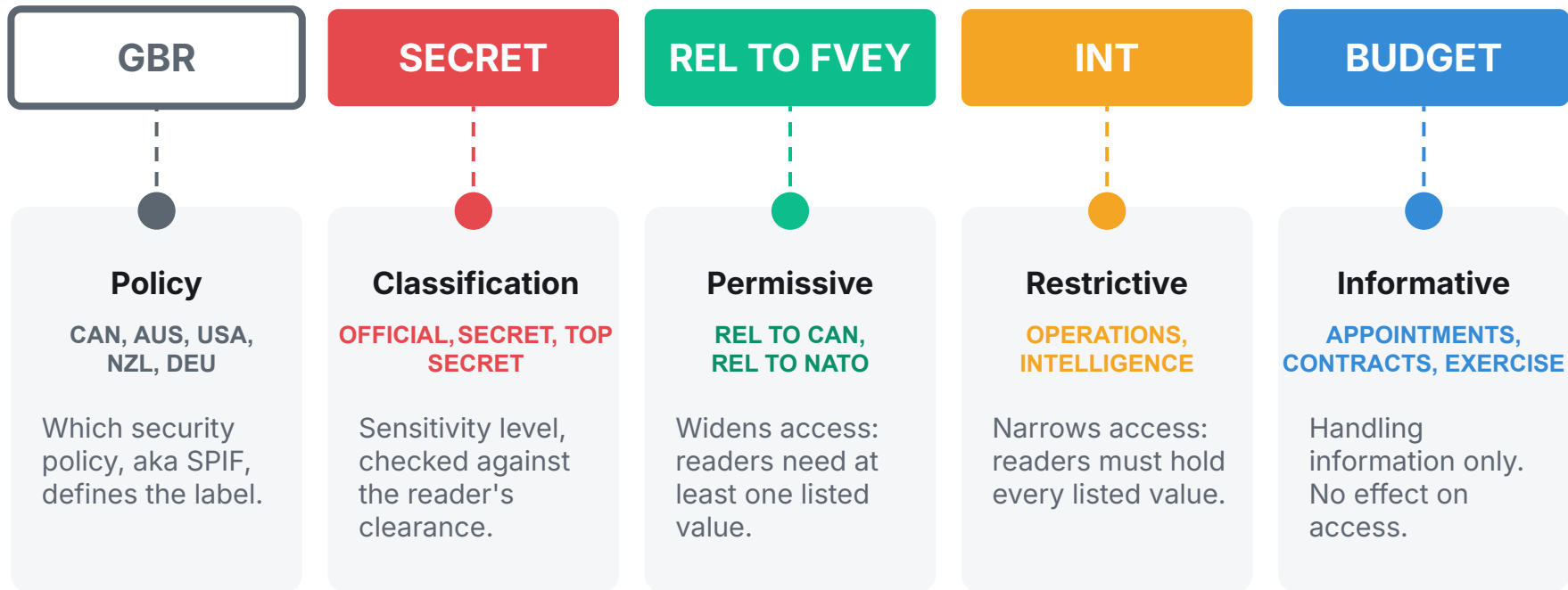
  <securityCategoryTag type="restrictive"
    name="Designators">
    <tagCategory name="INT"/>
  </securityCategoryTag>

  <securityCategoryTag name="Admin Marking">
    <tagCategory name="BUDGET"/>
  </securityCategoryTag>
</securityPolicyId>
```

SPIF /xml

ADatP /4774.1

# Anatomy of a Label.



Policy

Label

Syntax

Room

Event

Client

Server

# Clearance and Classification.

GBR

SECRET

REL TO FVEY

INT

BUDGET



**John Smith**

Clearance  
**SECRET**

Nationality  
**DEU**

Need-to-know  
-

**ID**

**Classification**

SECRET label, SECRET clearance



**Permissive**

Releasable to FVEY, John is DEU



**Restrictive**

John does not hold INT Need-to-Know



**Informative**

BUDGET: no access check



**Access Denied:** Nationality and Restrictive clearance checks would fail.

Policy

Label

Syntax

Room

Event

Client

Server

# Clearance and Classification.

**GBR****SECRET****REL TO FVEY****INT****BUDGET****Jane Doe**

Clearance

**TOP SECRET**

Nationality

**USA**

Need-to-know

**INT, OPS****ID****Classification**

SECRET label, up to TOP SECRET clearance

**Permissive**

Releasable to FVEY, Jane is USA

**Restrictive**

Jane holds INT Need-to-Know

**Informative**

BUDGET: no access check

**Access Granted:** Every check passes, Jane is cleared to see the message

Policy

**Label**

Syntax

Room

Event

Client

Server

# Labelling Syntax.

SPIF /xml

```
<securityPolicyId name="GBR">
  <securityClassification name="OFFICIAL" lacv="3"/>
  <securityClassification name="SECRET" lacv="4"/>
  <securityClassification name="TOP SECRET" lacv="5"/>

  <securityCategoryTag enumType="permissive"
    name="Releasable To">
    <tagCategory name="FVEY"/>
    <tagCategory name="NATO"/>
  </securityCategoryTag>

  <securityCategoryTag type="restrictive"
    name="Designators">
    <tagCategory name="INT"/>
    <tagCategory name="OPS"/>
  </securityCategoryTag>

  <securityCategoryTag name="Admin Marking">
    <tagCategory name="BUDGET"/>
    <tagCategory name="STAFF"/>
  </securityCategoryTag>
</securityPolicyId>
```

ADatP /4774.1

GBR

SECRET

REL TO FVEY

INT

BUDGET

CMLS /xml

```
<originatorConfidentialityLabel>
  <ConfidentialityInformation>
    <PolicyIdentifier>GBR</PolicyIdentifier>
    <Classification>SECRET</Classification>

    <Category TagName="Releasable To" Type="PERMISSIVE">
      <GenericValue>FVEY</GenericValue>
    </Category>

    <Category TagName="Designators" Type="RESTRICTIVE">
      <GenericValue>INT</GenericValue>
    </Category>

    <Category TagName="Admin Marking" Type="INFORMATIVE">
      <GenericValue>BUDGET</GenericValue>
    </Category>
  </ConfidentialityInformation>
</originatorConfidentialityLabel>
```

ADatP /4774.5

Policy

Label

Syntax

Room

Event

Client

Server

# Labelling Syntax.

GBR

SECRET

REL TO FVEY

INT

BUDGET

```

<originatorConfidentialityLabel>
  <ConfidentialityInformation>
    <PolicyIdentifier>GBR</PolicyIdentifier>
    <Classification>SECRET</Classification>

    <Category TagName="Releasable To" Type="PERMISSIVE">
      <GenericValue>FVEY</GenericValue>
    </Category>

    <Category TagName="Designators" Type="RESTRICTIVE">
      <GenericValue>INT</GenericValue>
    </Category>

    <Category TagName="Admin Marking" Type="INFORMATIVE">
      <GenericValue>BUDGET</GenericValue>
    </Category>

  </ConfidentialityInformation>
</originatorConfidentialityLabel>
  
```

CMLS /xml

ADatP /4774.5

GBR

SECRET

REL TO FVEY

INT

BUDGET

```

{
  "pol": "GBR",
  "cls": "SECRET",
  "catl": [
    {
      "type": "P", "name": "Releasable To",
      "vals": ["FVEY"]
    },
    {
      "type": "R", "name": "Designators",
      "vals": ["INT"]
    },
    {
      "type": "I", "name": "Admin Marking",
      "vals": ["BUDGET"]
    }
  ]
}
  
```

CMLS /json

ADatP /4774.7

Policy

Label

**Syntax**

Room

Event

Client

Server

# Labelling Syntax.

## From Rulebook to Label.

- The **SPIF** defines what's allowed for a policy

XML SPIF 2.1, ADatP-4774.1

- CMLS XML** records one specific label in XML

ADatP-4774.5

- CMLS JSON** is that same label defined in JSON

ADatP-4774.7

GBR

SECRET

REL TO FVEY

INT

BUDGET

CMLS /json

```
{
  "pol": "GBR",
  "cls": "SECRET",
  "catl": [
    {
      "type": "P", "name": "Releasable To",
      "vals": ["FVEY"]
    },
    {
      "type": "R", "name": "Designators",
      "vals": ["INT"]
    },
    {
      "type": "I", "name": "Admin Marking",
      "vals": ["BUDGET"]
    }
  ]
}
```

ADatP / 4774.7

Policy

Label

Syntax

Room

Event

Client

Server

# Labelling a Room.

## From Label to Matrix State Event.

- **spif** Reference to the SPIF stored in the media repo
- **spif\_hashes** SHA-256 of the SPIF, so tampering is detectable
- **max\_labels** Most restrictive label allowed in the room
- **default\_labels** What the composer picks by default

GBR

SECRET

REL TO FVEY

INT

BUDGET

```
{
  "type": "m.security_labels",
  "state_key": "",
  "content": {
    "spif": "mxc://example.org/spif-gbr",
    "spif_hashes": {"sha256": "vOSRYkr4..."},
    "max_labels": {
      "pol": "GBR", "cls": "SECRET",
      "catl": [
        {"type": "P", ... , "vals": ["FVEY"]},
        {"type": "R", ... , "vals": ["INT"]},
        {"type": "I", ... , "vals": ["BUDGET"]}
      ]
    }
  },
  "default_labels": {
    "pol": "GBR", "cls": "SECRET", "catl": [...]
  }
}
```

Unstable Prefix /io.element.security\_labels

Policy

Label

Syntax

Room

Event

Client

Server

# Labelling an Event.

## From Label to Matrix Event.

- m.security\_labels

Contains the **CMLS JSON** for the specific label of the message / event.

- spif

Reference to the SPIF stored in the media repo

- spif\_hashes

SHA-256 of the SPIF, so tampering is detectable

GBR

SECRET

REL TO FVEY

INT

BUDGET

```
{
  "type": "m.room.message",
  "content": {
    "msgtype": "m.text",
    "body": "hello",
    "m.security_labels": [{
      "label": {
        "pol": "GBR", "cls": "SECRET",
        "catl": [
          { "type": "P", ... , "vals": ["FVEY"] },
          { "type": "R", ... , "vals": ["INT"] },
          { "type": "I", ... , "vals": ["BUDGET"] }
        ]
      },
      "spif": "mxc://example.org/spif-gbr",
      "spif_hashes": { "sha256": "vOSRYkr4..." }
    ]
  },
  "spif": "mxc://example.org/spif-gbr",
  "spif_hashes": { "sha256": "vOSRYkr4..." }
}
```

Unstable Prefix /io.element.security\_labels

Policy

Label

Syntax

Room

Event

Client

Server

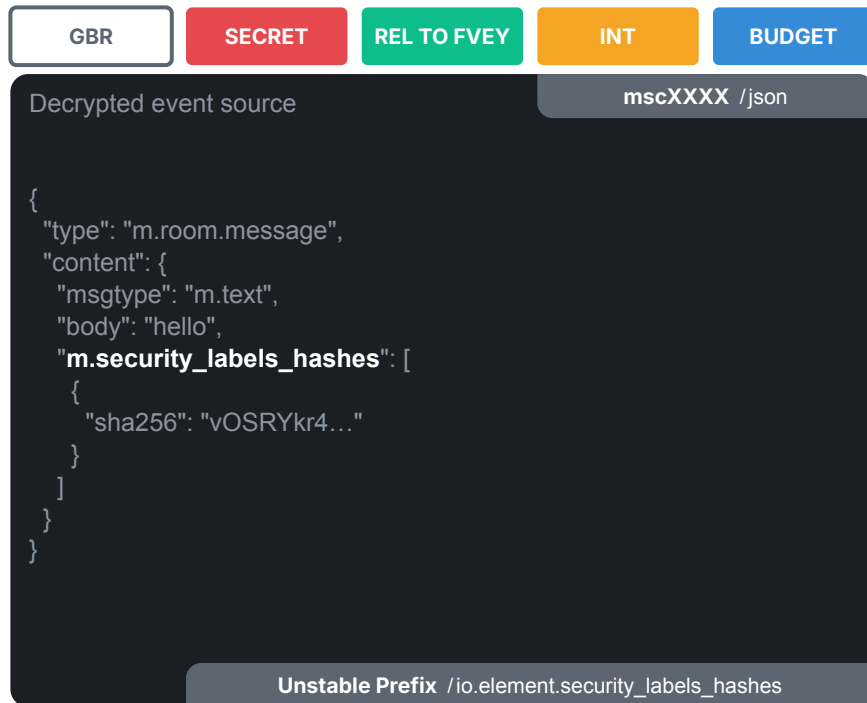
# Labelling an Event.

## From Label to Matrix Event.

When sending a labelled event in an encrypted room we also include a hash of the labels.

- `m.security_labels_hashes`

Contains the labels hash which can be used to check the labels outside the encryption haven't been tampered with.



Policy

Label

Syntax

Room

Event

Client

Server

# Sending Labels.

Which labels can be sent in this room?



✓ **Allowed:** Sent event label matches the max label



✓ **Allowed:** Informative tags don't affect access



✓ **Allowed:** Broader than restrictive INT



✗ **Rejected:** Not releasable to Five Eyes room members



**Restrictive tags narrow the audience and permissive tags widen it**

As such a message can drop a restriction but never a release.



# Built as an element-web module.

Single JavaScript  
bundle loaded at  
runtime



Policy

Label

Syntax

Room

Event

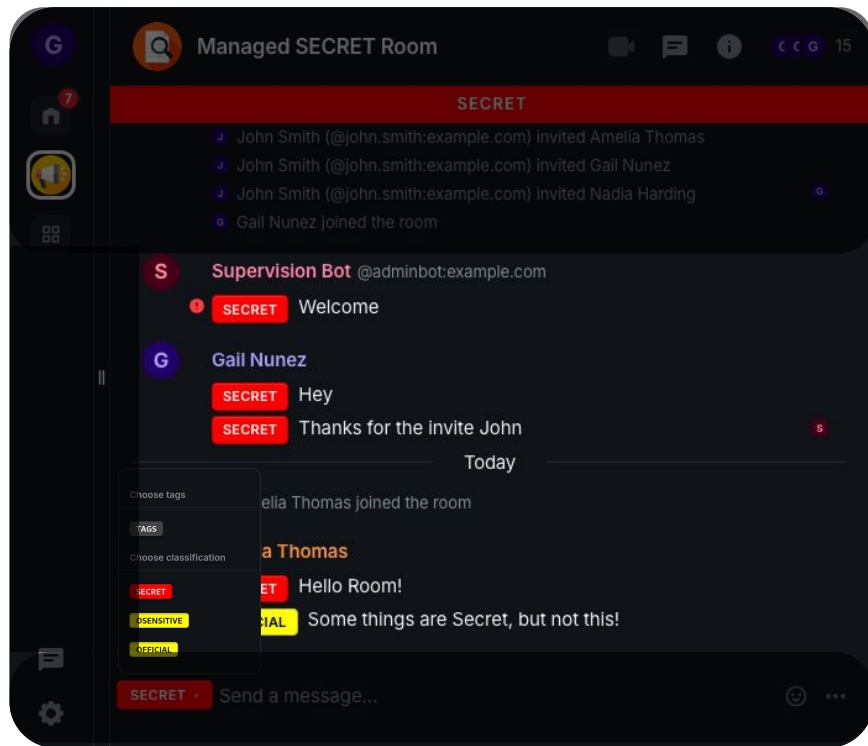
**Client**

Server

# Feature set.

## What does the module do?

- Associate a SPIF with a room via the room settings.
- Shows a room banner with the max label.
- Shows a component next to the composer which allows selecting the classification for a message.
- Can be configured to allow tag selection on a per room basis or a per message basis.
- Messages in the timeline are decorated with security labels.



Policy

Label

Syntax

Room

Event

Client

Server

# What we added.



## UI Components

- React components built in the MVVM style



## Security Label Store

- Downloads and parses SPIFs
- Computes the hashes of the SPIF and labels
- Builds the event labels



## Module API Additions

- Custom module settings
- New rendering APIs
- Message content transformation
- Media repository access

Policy

Label

Syntax

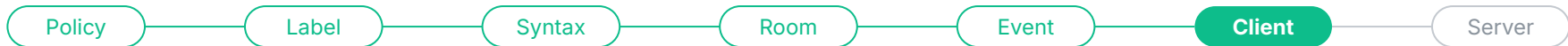
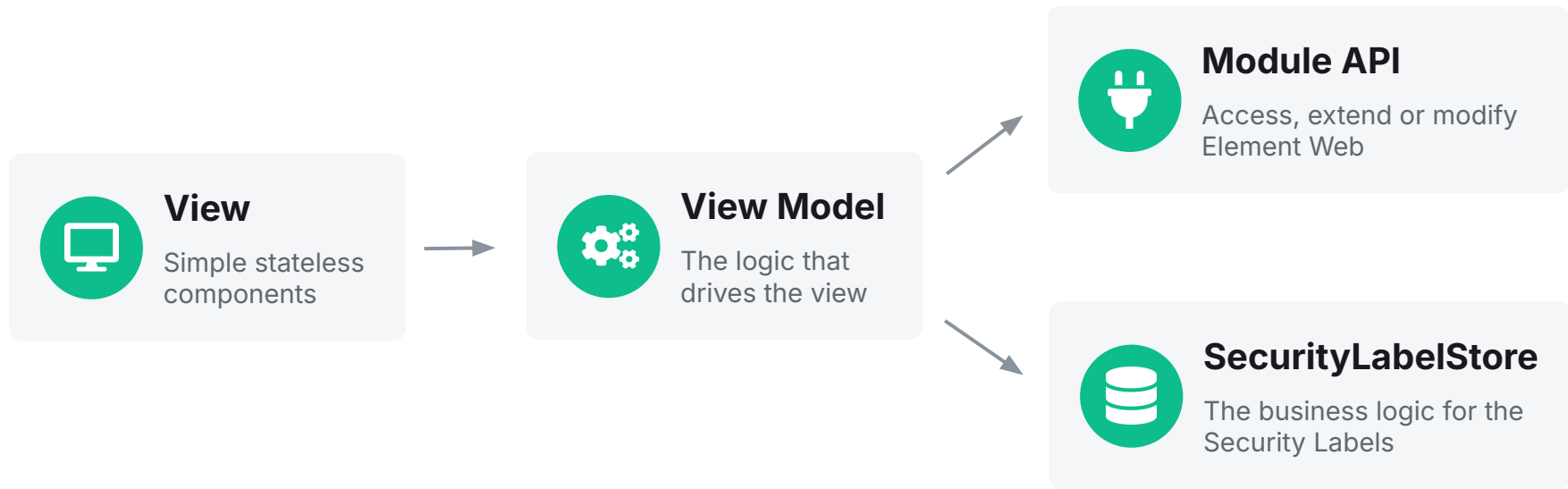
Room

Event

**Client**

Server

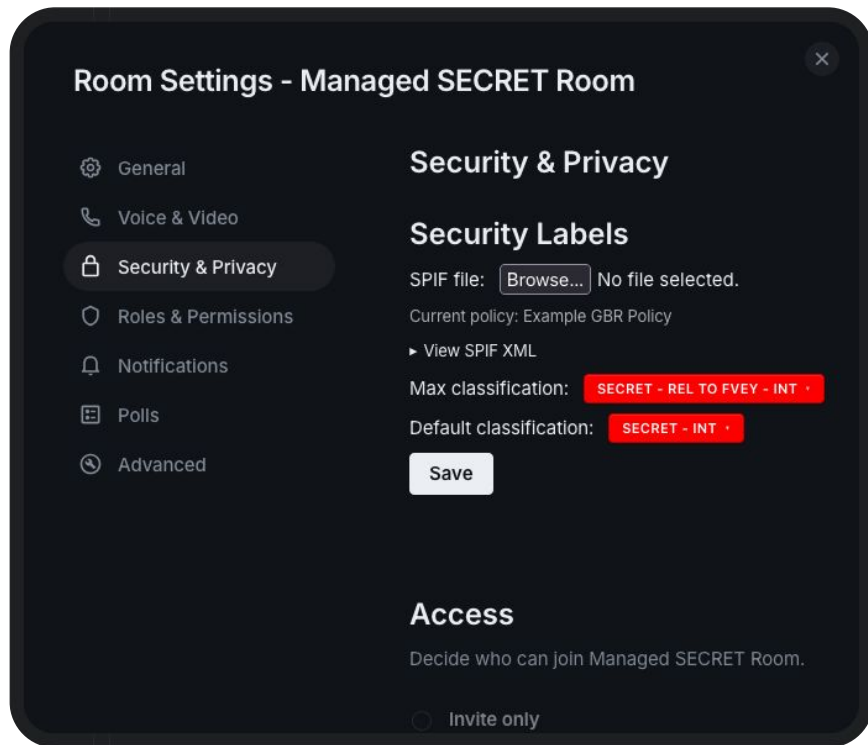
# Architecture.



# Architecture.

## Security label settings for a room.

1. **View** The save button. No logic, no state.
2. **View Model** The click calls methods on vm, for example, vm.save().
3. **Store** Builds the state event, as per the MSC.
4. **Module API** Set as state event on the room.



Policy

Label

Syntax

Room

Event

Client

Server

# Policy Enforcement.



## Preventive

PEP

Synapse MPE module

Room Joins, Message Sends



## Corrective

PEP

AIAM bot in the room

Continued Room Membership



## Authoritative

PDP

OpenTDF

Decisions based on Policies

## Access control is split into two roles:

- Policy Enforcement Point (**PEP**)

Asks for a decision and enforces the answer

For example, Synapse and AIAM

- Policy Decision Point (**PDP**)

Holds the policy and makes the permit or deny decision.

For example, OpenTDF

Policy

Label

Syntax

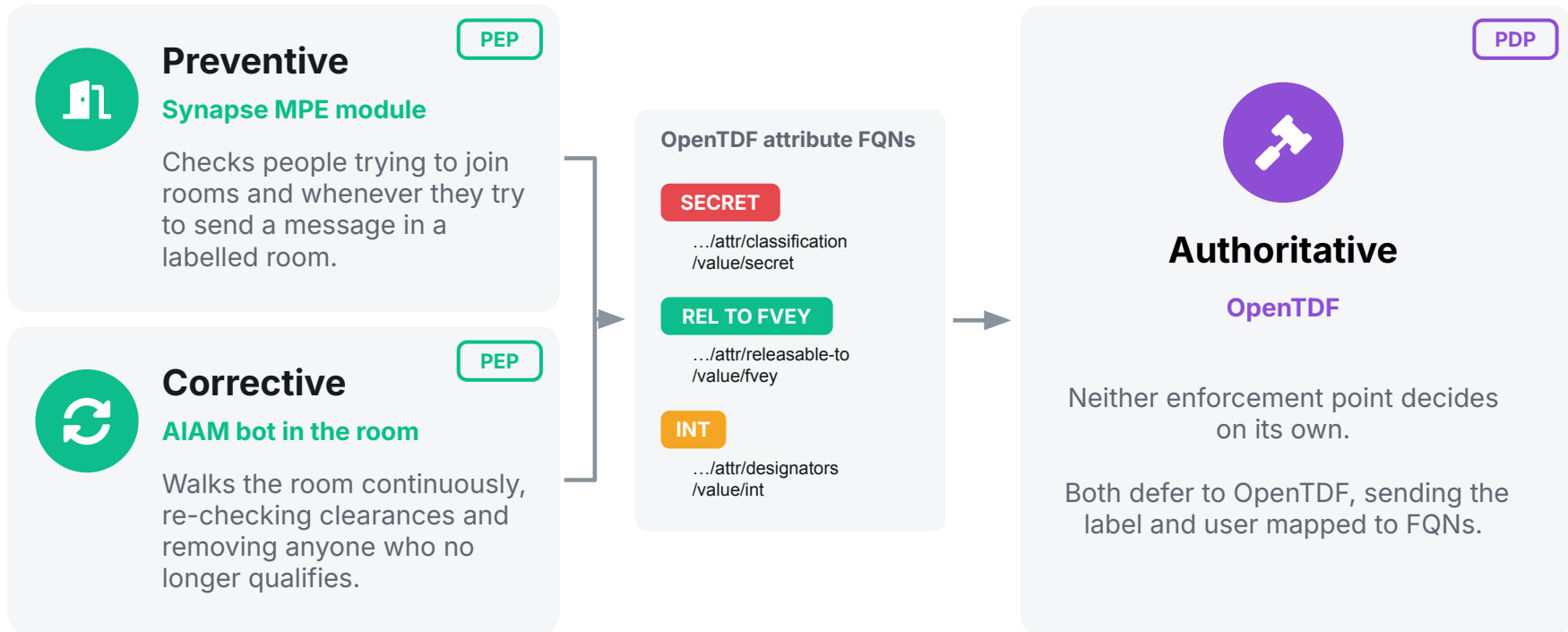
Room

Event

Client

Server

# Policy Enforcement.



Policy

Label

Syntax

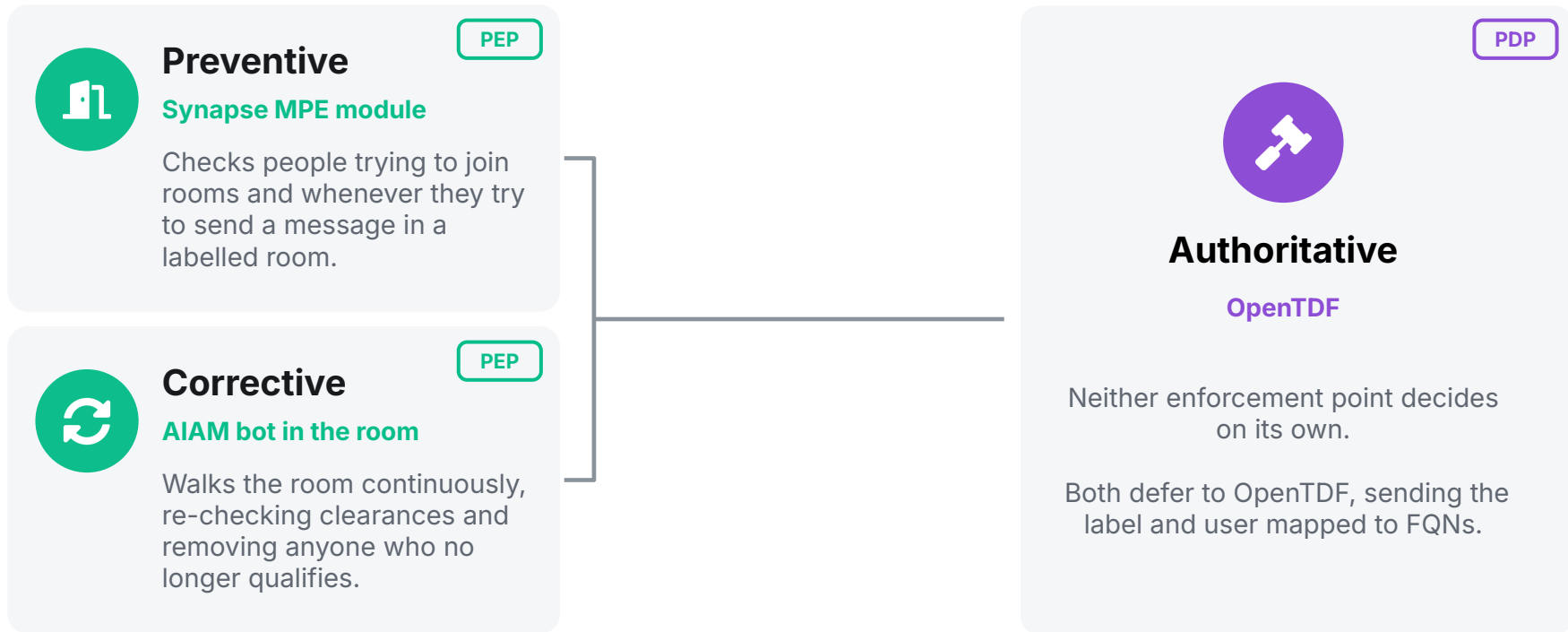
Room

Event

Client

Server

# Policy Enforcement.



# Demo.

# What's Next?

**Descoped for now, left for future MSCs:**

- Mapping equivalent labels between SPIFs
- Multiple SPIFs in one room
- Full STANAG 4778 binding data objects

# Questions?

GBR

SECRET

REL TO FVEY

INT

BUDGET