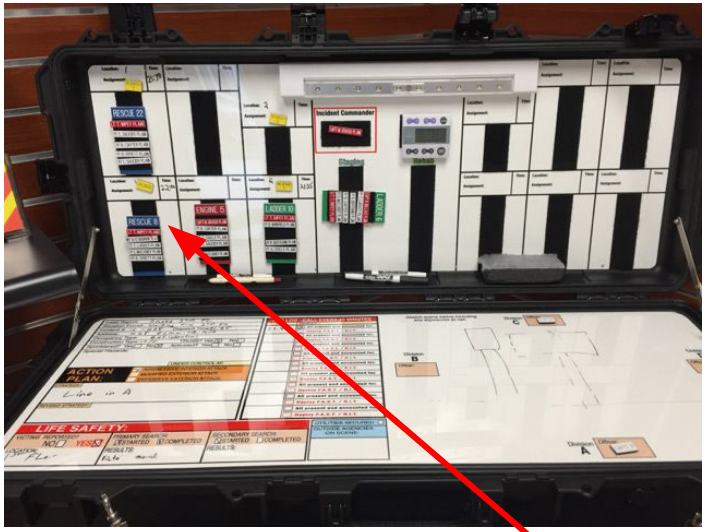
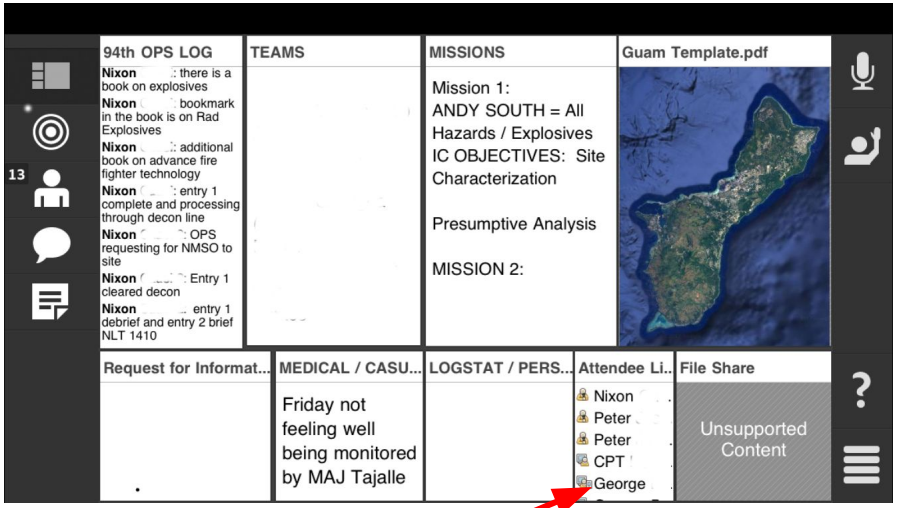
ERASMUS

Emergency Responder Authentication System for Mobile Users

Old tools / New tools: Same challenge





Who are these people?
Non-scalable IDM process

Disaster strikes… we need people to help?

Who are you?

What skills do you have?

Are you authorized to be here?

… x 1000 people

Challenge

The emergency responder ecosystem in the US is highly decentralized--there are thousands of organizations, with hundreds of thousands of affiliated people. There is currently **no universal, interoperable identity infrastructure**.

- Smart cards are difficult to issue, update, and revoke--barriers are too high for wide adoption.
- Mobile is the answer, but where would the information come from? There is no central database of emergency responders.

Impact of Failure - we should cost this out (at some point)

Without an identity infrastructure, the next wave of applications are stuck in the mud

- Event management systems
- Computer aided dispatch
- Payment Settlement
- Physical Access Control
- Next generation radio / location services / IOT

A Federation provides the “Tools and Rules”

The tools include standards and shared services.

The rules define a “trust framework” with the policies and operating procedures--enables this decentralized community to act based on appropriate levels of risk mitigation.

The ERASMUS Federation, an organization dedicated to serving emergency responders, will define the technical standards, schema, agreements and provide strategic centralized services, using next generation technology.

PILOT

Goals of 6-month pilot (February -August 2017)

1. **Minimum Viable Product**
   Create a mobile app that demonstrates the backend services of the federation.

2. **Community Feedback**
   Get input from emergency responders to guide future investment.

ERASMUS STANDARDS

OpenID Connect

1. OAuth 2.0 based identity layer
2. Provides API's for authentication and the release of user claims
3. Support for mobile and web applications
4. Draft federation standard adds stable signing keys

http://openid.net/connect/

Open Badges 2.0

1. Information-rich visual representations of verifiable achievements earned by recipients
2. Contain identity assertion
3. Can be used for non-connected use cases (“badge baking”)
4. Expressed as linked data (JSON-LD) so that badge resources can be connected

http://gluu.co/open-badges-2-0

Example: “Hazmat Technician”

Add face to make this real.


```
{"@context": "https://w3id.org/openbadges/v2",
  "id": "https://erasmus.dhs.gov/assertions/e8d341e8c70a",
  "type": "Assertion",
  "issuedOn": "2016-12-31T23:59:59+00:00",
  "verification": {"type": "hosted"},
  "recipient": {"type": "email",
                "identity": "alice@houston-fire.tx.gov"},
  "badge" {"type": "BadgeClass",
    "id": "https://erasmus.dhs.gov/badges/881efbf7ff58",
    "name": "HAZMAT Technician",
    "description": "Must attend an NFPA 472, 40 hour course designed for personnel who respond to emergencies involving Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD) for the purpose of analyzing the incident, selecting appropriate PPE and decontamination procedures, and implementing action options to mitigate the incident",
    "image": "https://erasmus.dhs.gov/badges/881efbf7ff58/image",
    "criteria": {"narrative": "Upon completion of this course you must successfully pass the National Board on Fire Service Professional Qualifications (Pro Board) written exam and skills testing for NFPA 472 Chapter 7."},
     "issuer": {"id": "https://erasmus.dhs.gov/",
      "type": "Profile",
      "name": "ERASMUS Federation",
      "url": "https://erasmus.dhs.gov/public",
      "email": "info@erasmus.dhs.gov",
      "verification": {"allowedOrigins": "erasmus.dhs.gov"}}}
```

Trust Marks

1. Machine-readable, cryptographically signed digital artifact that represents a statement of conformance to a well-scoped set of trust and/or interoperability requirements.
2. Enables organizations to convey security risk information. Answers the question: How good is the security of the organization that issues the credential?

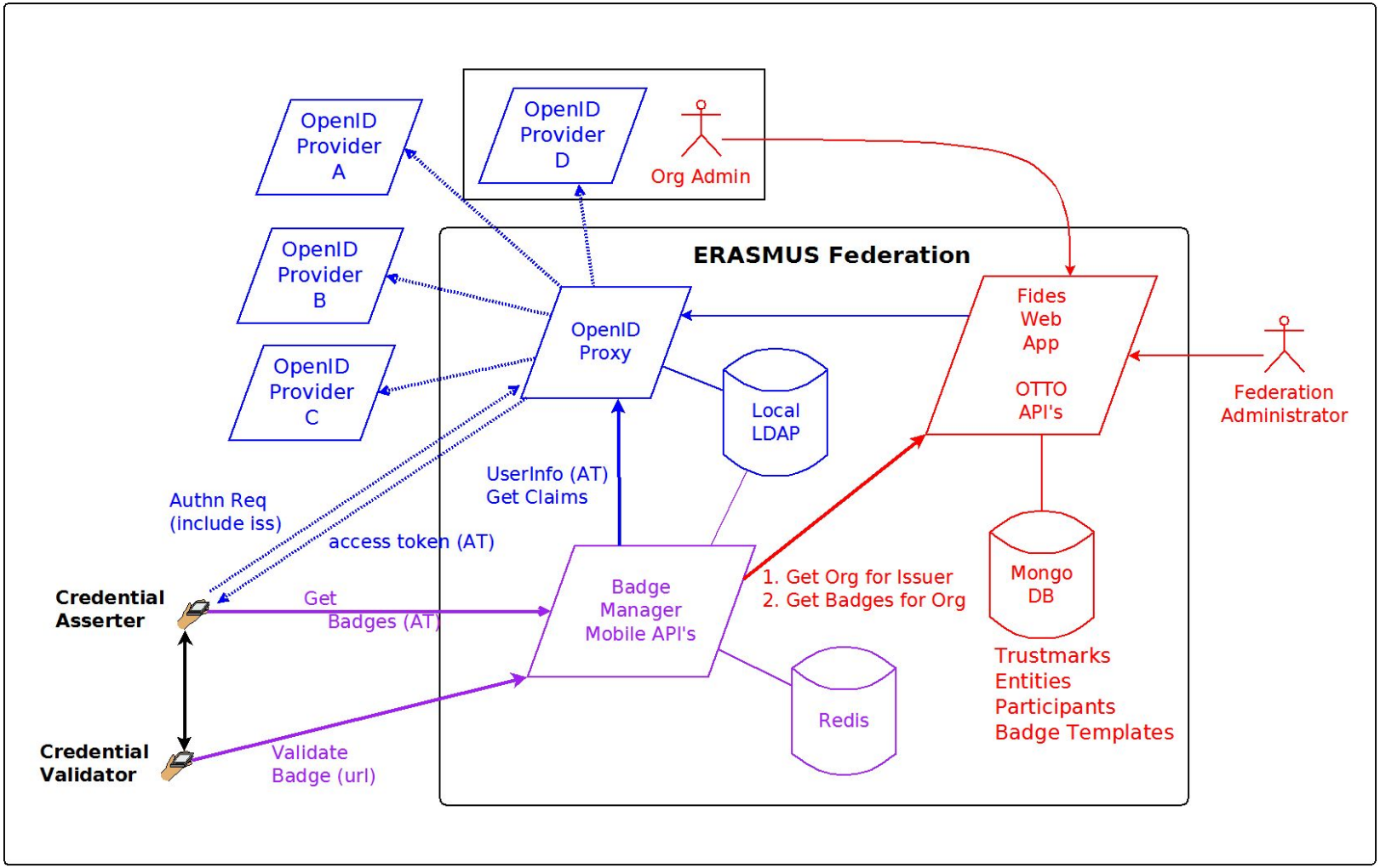
http://gluu.co/trustmark-spec

Kantara OTTO

1. API's and JSON-LD schema for multi-party federation management
2. Used to publish:
    a. public signing keys of each OpenID Provider
    b. Other metadata about federation participants
    c. Badge templates
    d. Standards for user claims
    e. Trust marks for participants

https://github.com/KantaraInitiative/wg-otto

ERASMUS Components

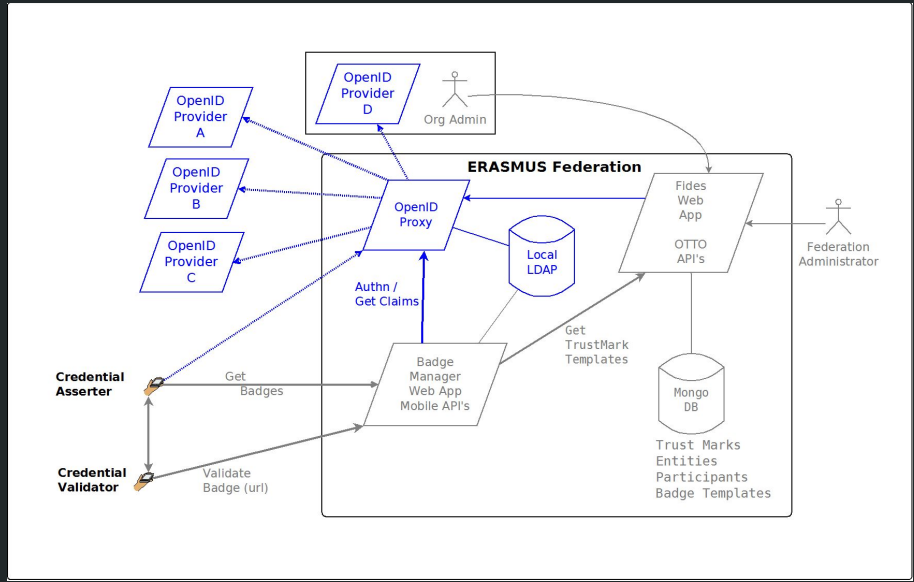

OpenID Provider A
OpenID Provider D
Org Admin
OpenID Provider B
OpenID Provider C
ERASMUS Federation
OpenID Proxy
Fides Web App
OTTO API's
Federation Administrator
Local LDAP
UserInfo (AT)
Get Claims
Authn Req
(include iss)
access token (AT)
Credential Asserter
Get
Badges (AT)
Badge Manager Mobile API's
1. Get Org for Issuer
2. Get Badges for Org
Mongo DB
Trustmarks
Entities
Participants
Badge Templates
Redis
Credential Validator
Validate
Badge (url)

Gluu Server

OpenID Provider

Can proxy authentication requests to backend OpenID Providers (OP)

Caches user claims from backend OP’s for quick retrieval

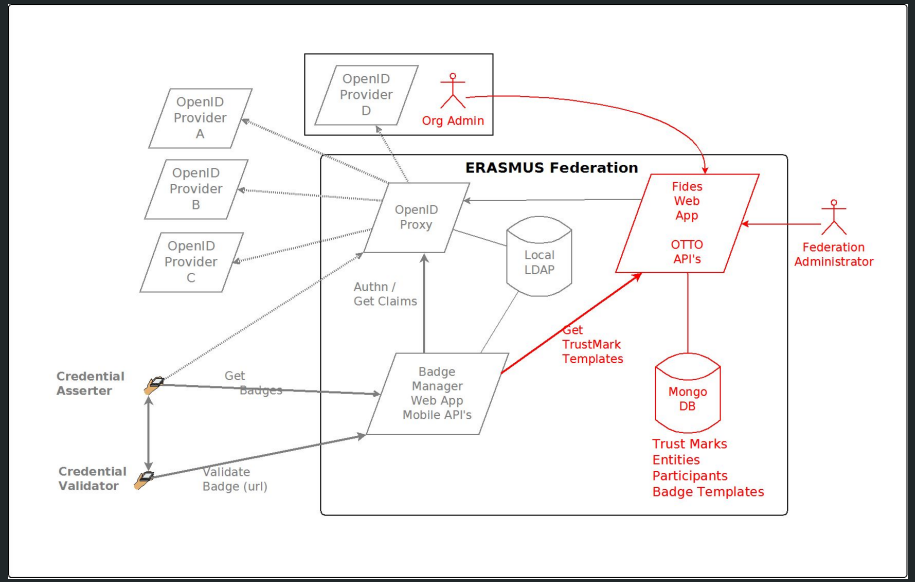


FIDES

Handles organization registration

Used by federation admins to approve membership applications

Publishes data using OTTO API’s and JSON-LD

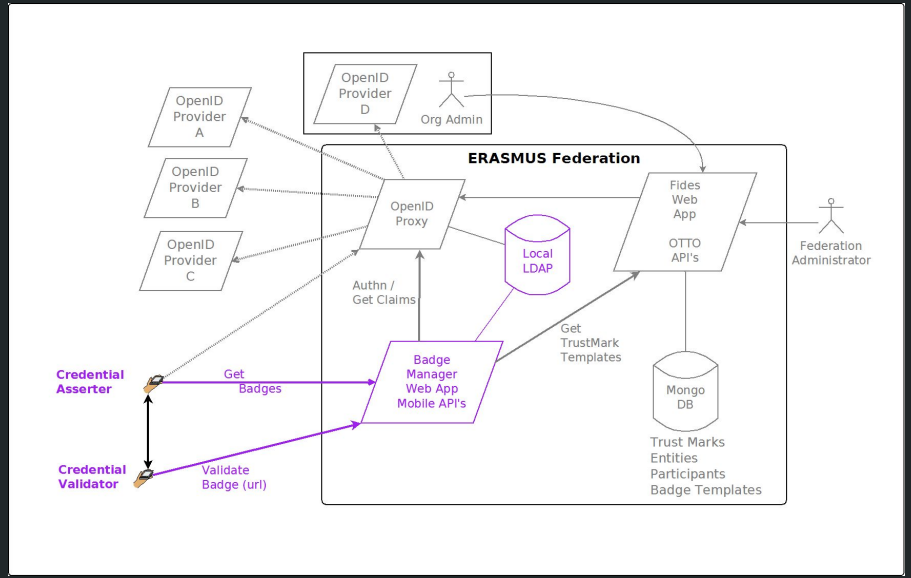


Badge Manager APIs

Publishes public URL’s for badge instances

Publishes temporary URL’s for badge instances (privacy protecting)

Commercial license



Mobile Application

Pilot: Android only (iOS phase II)

Login at home organization

Apply for Badge

Display Badge

Verify Badge

What would ERASMUS achieve?

Services will be able to digitally identify people and retrieve current information.

Local organizations will review and approve the issuance of badges.

Local revocation of credentials will be effective immediately.

ERASMUS will hold information about organizations, people, their skills, and location.

ERASMUS will have the ability to push notifications to registered devices.

This infrastructure will enable the construction of a next generation of identity aware digital services.