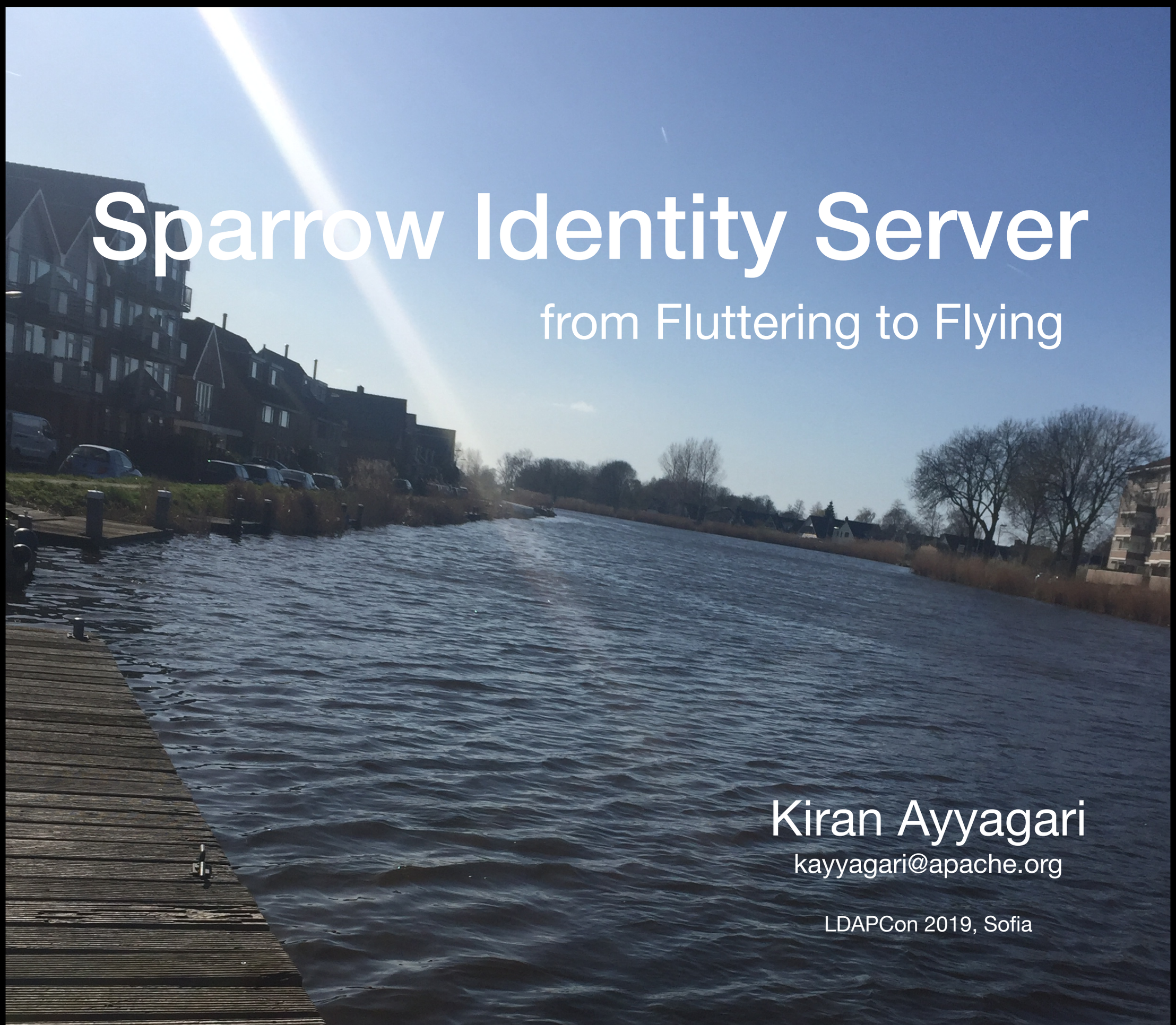
Sparrow Identity Server

from Fluttering to Flying



Kiran Ayyagari

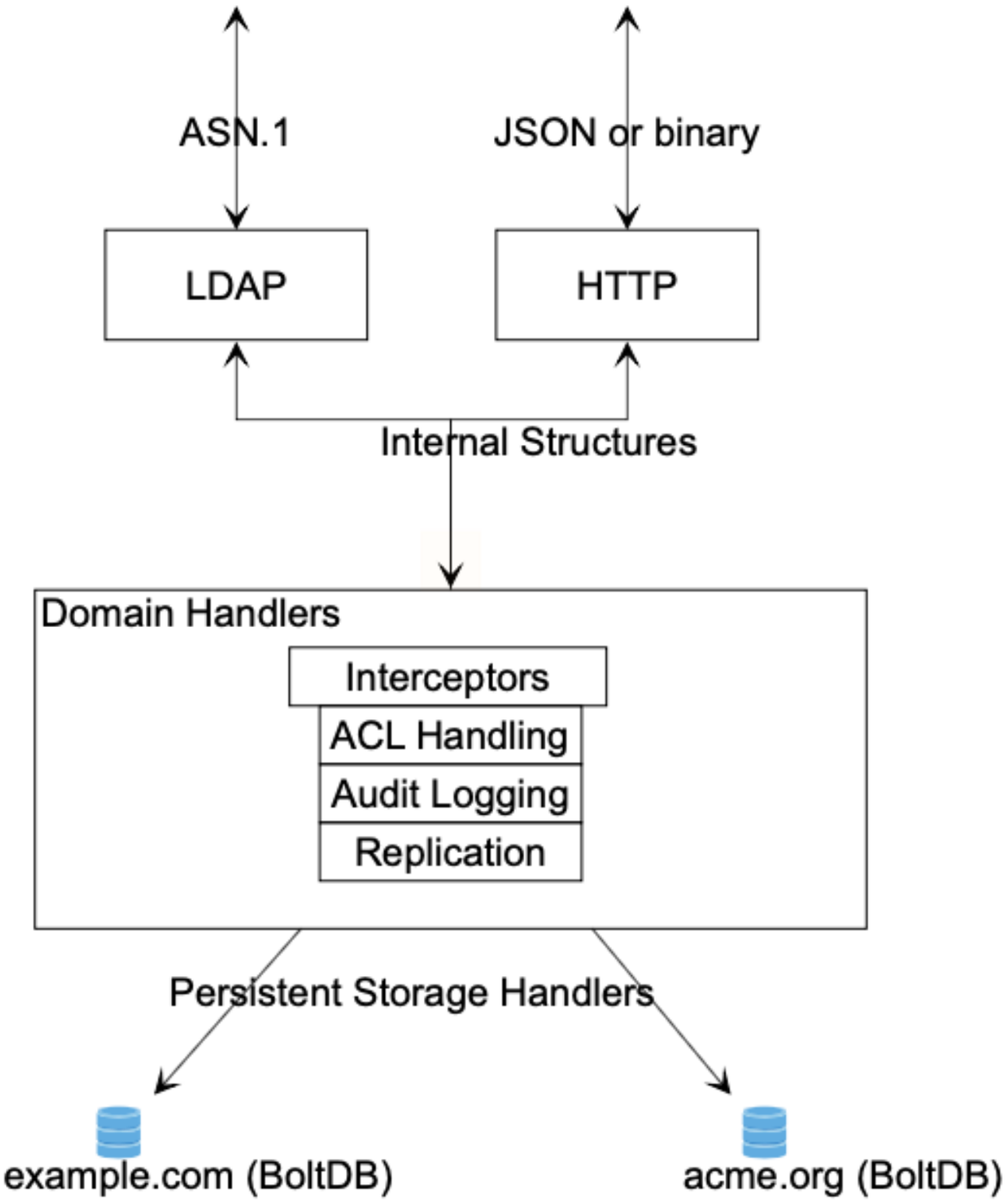
kayyagari@apache.org

LDAPCon 2019, Sofia

What is it?

- Identity Server
- Provisioning based on SCIMv2
- SSO using OpenIDConnectv2 and SAMLv2
- Supports LDAPv3 Bind and Search Operations
- 2FA using TOTP (over both HTTP and LDAP)
- Authenticate using Security Keys (a.k.a Webauthn)
- Supports Multi-Master replication over HTTPS

Architecture Overview



Access Control

Is based on

- User’s group membership
- Entry(a.k.a Resource) Attributes
- Entry Filters

ACLs are stored in each group entry

Example of permissions for a group on “User” Resource:

```
[
    {
        "allowAttrs": “*", // wildcard support
        "filter": “ANY", // ANY is a special marker filter
        "op": “read"
    },
    {
        "allowAttrs": “lastName, firstName, email”, // CSV of attribute names
        "filter": “(userType EQ \”Contractor\”)“, // filter can be any valid SCIM2 resource filter
        "op": "write"
    }
]
```

Audit Logging

- AuditEvent is modeled as a SCIMv2 Resource
- The events are backed by a schema
- Searchable using SCIM filters

Example entry:

{ "actorId": "00000000-0000-4000-4000-000000000000",

"actorName": “admin",

"desc": "Searched for resources of type Group",

"ipAddress": "127.0.0.1:49885", "operation": "Search",

"payload": "", "statusCode": 200, "uri": "/Groups" }

Authentication

- 2FA using TOTP over both HTTP and LDAP
- Supports Webauthn for signing-in with Security Keys

What is Webauthn?

- Web Authentication
- An API for accessing Public Key Credentials
- W3C Recommendation
- Supported by all major Web Browsers
- Phishing Resistant

Demo time…

Replication

- Zero-conf setup
- Peer to Peer (over HTTPS)
- Peer1’s admin sends a Join request
- Peer2’s admin approves the Join request
- Replication begins

Deployment Options

- As a plugin of Caddy web server (default)
- Behind a reverse proxy (NGINX, httpd etc.,)

What Next?

- Join a replication cluster of N peers with single Join request
- OpenIDConnect Certification
- Improve the administrator dashboard web-app
- Integrate with Heimdal (Sparrow will be the backend)
- Audit-log aggregation

Thank You

Emmanuel Lécharny
elecharny@apache.org

Shawn McKinney
smckinney@symas.com