RED HAT
FORUM
Europe, Middle East & Africa

redhat.

BUILD YOUR OWN CLOUD ON CUSTOMER SIDE

A STORY ABOUT DESIGNING AN OPEN SOURCE HYBRID CLOUD ACCESS SECURITY BROKER

SÉBASTIEN PASCHE

SENIOR ARCHITECT

ELCA INFORMATIK AG

Who am I

I ’am a computer security enthusiast
Security contests, Malware, Web architecture

Open source contributor since 2001

Volunteer in multiple organizations

Addict to absurd & abstract arts

Sebastien Pasche
Twitter @braoru
@ELCA since 01.2017
Architect @leshop 2012-2017
Freelance (mainly biomed) Architect 2006-2017

“The corollary of constant change is ignorance. This is not often talked about: we computer experts barely know what we’re doing. We’re good at fussing and figuring out. We function well in a sea of unknowns. Our experience has only prepared us to deal with confusion. A programmer who denies this is probably lying, or else is densely unaware of himself.”

Ellen Ullman, Close to the Machine: Technophilia and Its Discontents

AGENDA

A few word about ELCA position in swizerland

Current SAAS externalization problematics

The CloudTrust project and the “CASB” word

Current status and technical issues we are facing

A few word about crypto and searchable encryption

Founded in 1968

Over 800 employees

Turnover of CHF 118.8 millions in 2016 (growth 11%)

1‘000 customer projects in ten years

Cloud and problems

ELCA and cloud migration projects

ELCA conducted lot of cloud migration related project

- More than 100 (IDaaS, IAM , IGA, User Management Process) projects
- Infrastructure migration
- Developing private clouds for ELCA and customers

Mainly involved in design and integration of commercial product

Currently ELCA don’t create cloud enabler software

Want to go to the cloud but you are located in Swizerland ?

What could go wrong

Data privacy
Ensure that sensible information are not disclosed

Access & location
Keep control over data access and its location

B2B collaboration
Allow secure collaboration with B2B while keeping lower costs

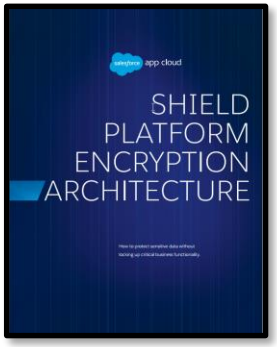
Compliance
Ensure compliance with legal regulations

Who control your encryption keys and your identities ?

When you protect content with Azure RMS, Azure RMS uses a 2048-bit RSA asymmetric key with SHA-256 hash algorithm for integrity to encrypt the content. The symmetric key for Office documents and email is AES 128-bit (CBC mode with PKCS#7 padding).

In a default Azure RMS implementation, Microsoft generates and manages the root key that is unique for each tenant. Customers can manage the lifecycle of their root key in Azure RMS with SharePoint Online by using a method called Bring your Own Key (BYOK) that allows you to generate your key in on-premises HSMs, and stay in control of this key after transfer to Microsoft's FIPS 140-2 Level 2-validated HSMs. Access to the root key is always limited to Office 365 applications (such as Exchange Online and SharePoint Online) and is not given to any personnel. In addition, customers can access a near real-time log showing all access to the root key at any time. For more information, see Logging and Analyzing Azure Rights Management Usage.

Source : Data Encryption Technologies in Office 365



Shield Platform Encryption allows Salesforce administrators to manage the lifecycles of their data encryption keys while protecting the keys from unauthorized access. To ensure this level of protection, data encryption keys are never persisted on disk. Instead, they're derived on demand from the master and tenant secrets.

The master secret is generated by a master HSM at the start of each release. The master HSM is "air-gapped" from Salesforce's production network and stored securely in a bank safety deposit box. Only designated Salesforce security officers can access the safety deposit box and the master HSM stored within.

Current ELCA customers's concerns

No Vendor lock-in

Keep you own keys approach (KYOK)

Flexibility between on-premise and SAAS design

Replace assembly of multiple complex products by an unified approach

Expertise on integration and help with process and strategy

Transparency on how it's working and what we are doing with data (can be audited anytime)

High availability on a large multi-cluster scale


CloudTrust

Coudtrust as an ELCA opensource project

3 friends active in the ”cloud” industries dealing with the same problems..

Licensing model of the market don’t fit mid sized Swiss company

Lack of open source alternatives or complex setup to build not suited for low OPEX approach

ELCA is a company designing and integrating cloud solution within lot of customers in Switzerland

ELCA own a great DEV power and own their own Swiss based cloud for critical hosting

ELCA don’t have an in-house global solution

01.01.2017 we decided to put our effort in common and start the development of an **opensource** CASB solution internally at ELCA

Technical busniess axes

Access

SSO, ABAC, Access policy, MFA

Visibility, Compliance

Manage

B2E, B2B, B2C, Users provisioning, Workflow, Branding

Visibility, Compliance

Control

Shadow IT, License metering, behavior analytics, reporting

Visibility, Compliance, Threats protection

Protect

Field Protection, Searchable encryption, Proxy/Reverse

Threats protection, Data Loss Prevention

Cloudtrust technical vision

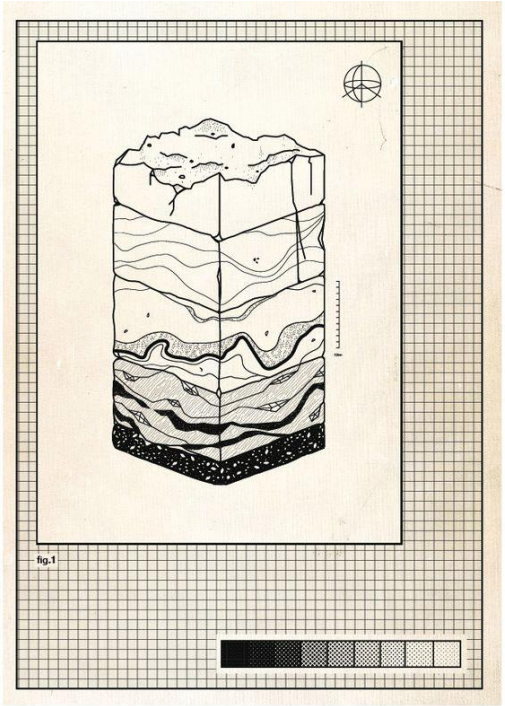
OpenSource and Transparent

Support multiple deployment target
    SAAS, Appliances, Customer hosted PAAS

Organized as a toolkit with dedicated distribution

Keep OPEX stable
    Multi tenancy, Use vanilla technologies,
    Use/Improve open source, clustering.

Embark other ELCA security project
    MFA, Crypto, ..



Cloud & appliance based

Appliance design

We target 3 runtime environments

On-premise, Customer PAAS, ELCA/public hosted SAAS

We must share technology and be compliant with the multiple target platforms

Use of standard technology and standard setup

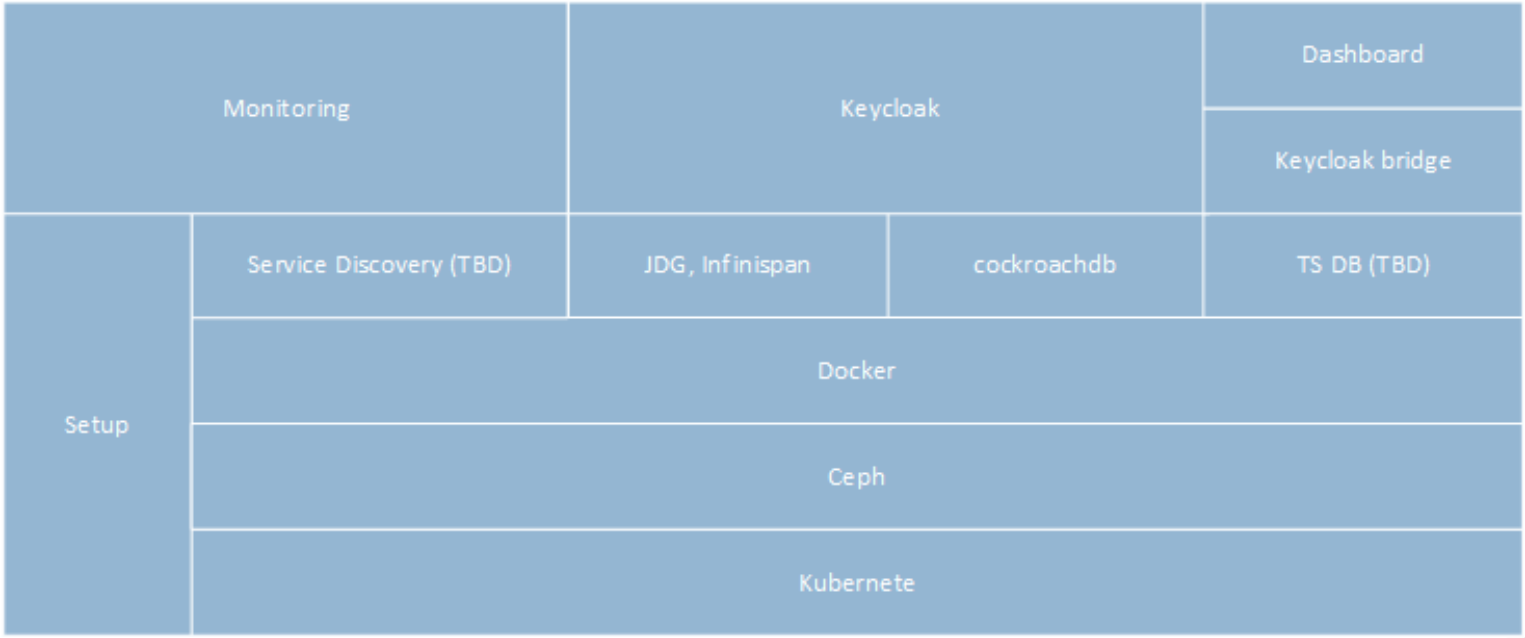
We must keep OPEX Cost stable

Use well-know technology, use technology easy to integrate within continuous deployment

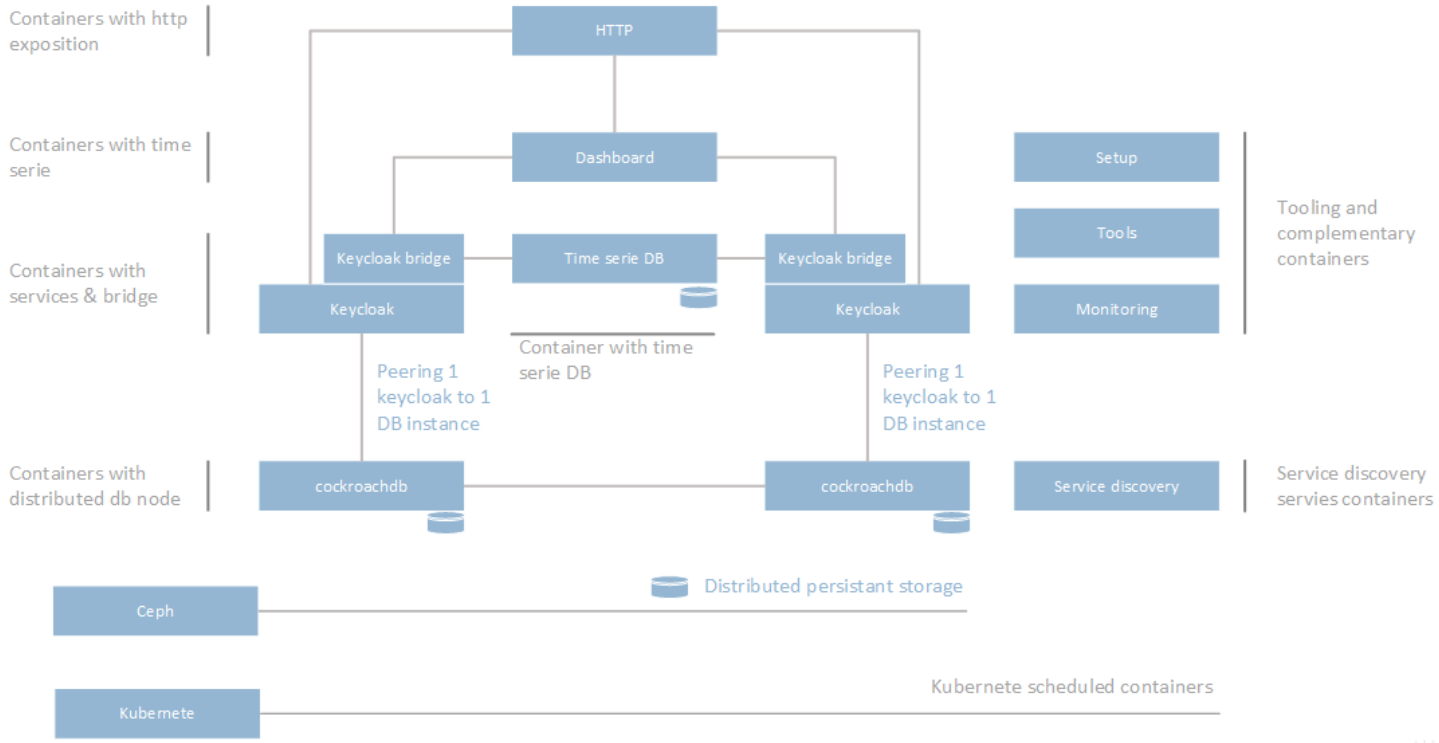
We must be able to split services between on-premise and cloud architecture

Kubernete federation is our current plan

Appliance design



Appliance design



Access and Manage

Keycloak

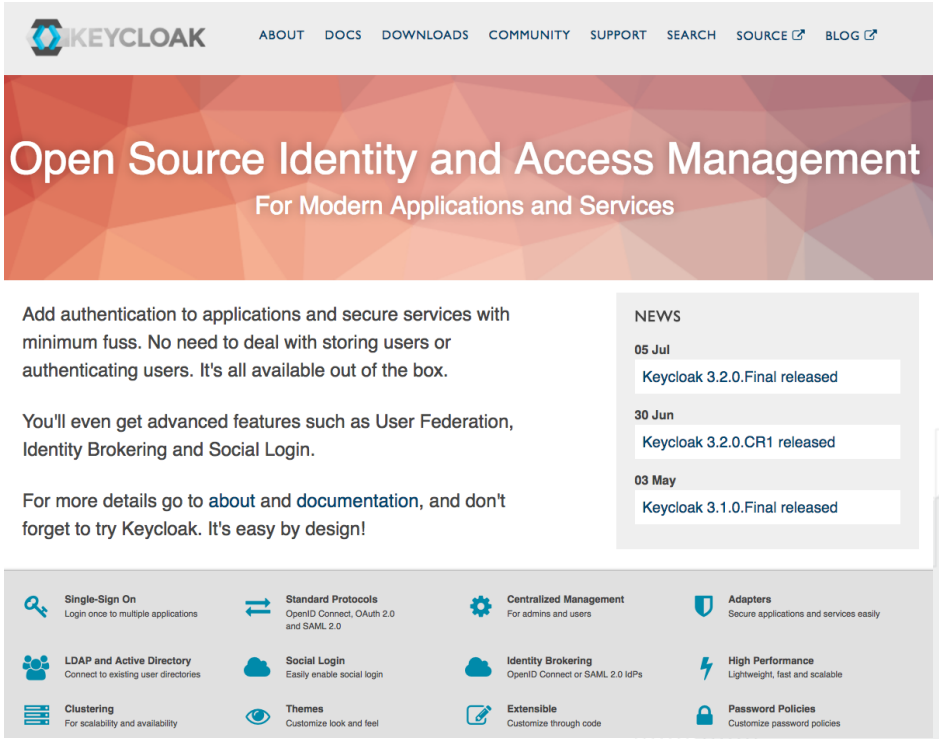
Offers most of required features

Clean codebase and architecture

Highly extensible and customizable
Modules, extensions, themes, …

Open source with possible redhat support

Documented and complete REST API



Current work with keycloak

Keycloak doesn’t support WS-FED out of the box

We started to create a module with the helps from “quest” and “agi.com”

https://github.com/cloudtrust/keycloak-wsfed

Active active multi-dc setup of keycloak is still moving

We are working with the community to extend cockroachdb support, design Infinipsan configuration and modules

Lack of log analysis and business metrics

We are working on a module to propagate keycloak event within a reactive ecosystems (POC validated)

Current work with keycloak

Lack of Dashboard and reporting

We created a pet services directly connected to keycloak events which will act as a busniess analysis providers

Lack authentication + secure channel creation

We planned to implement SRP authentication module for keycloak

Micro services compatible interfaces

We implementing a full keycloak GRPC API interface within our pet services

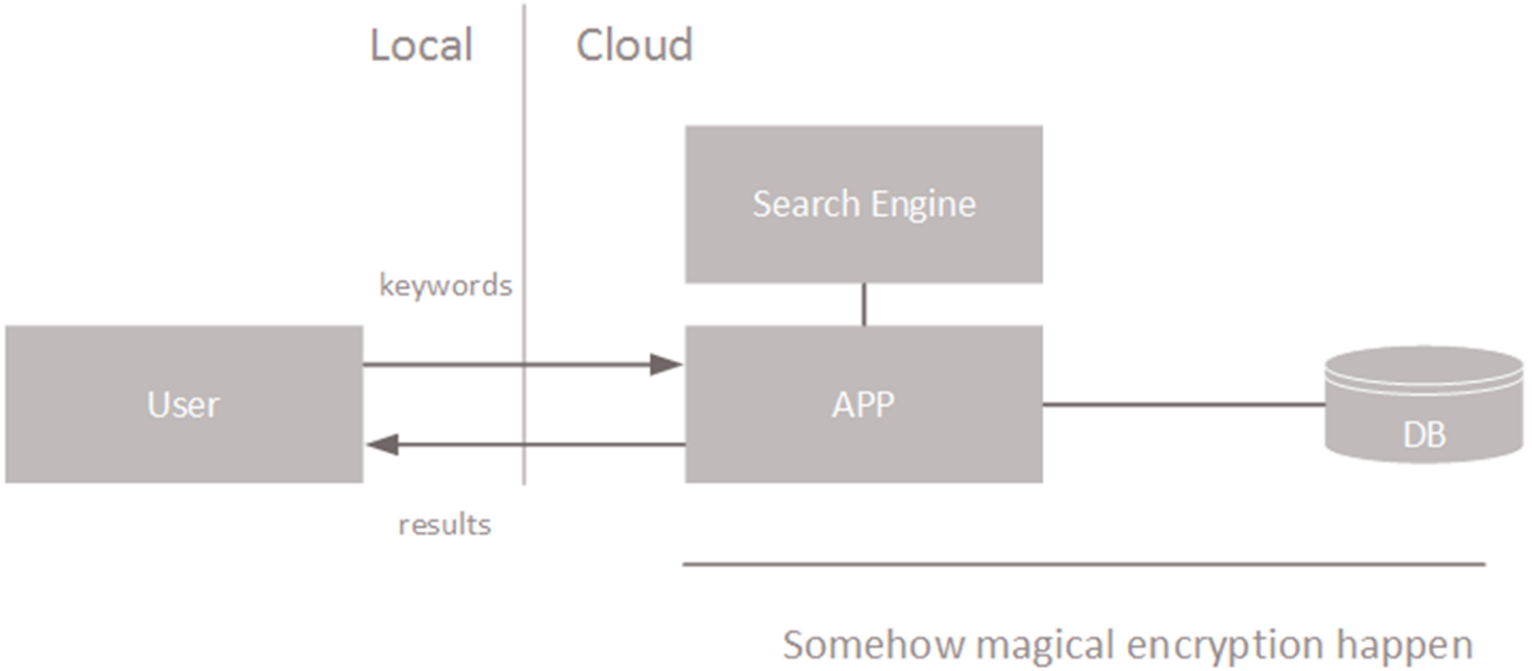
Protect

Searchable encryption, FPE, OPE ..

Most of the time, this is not exactly what you may imagine

Searchable encryption

What people imagine



Naïve Deterministic Word-Substitution Cipher

Do not preserve format & order

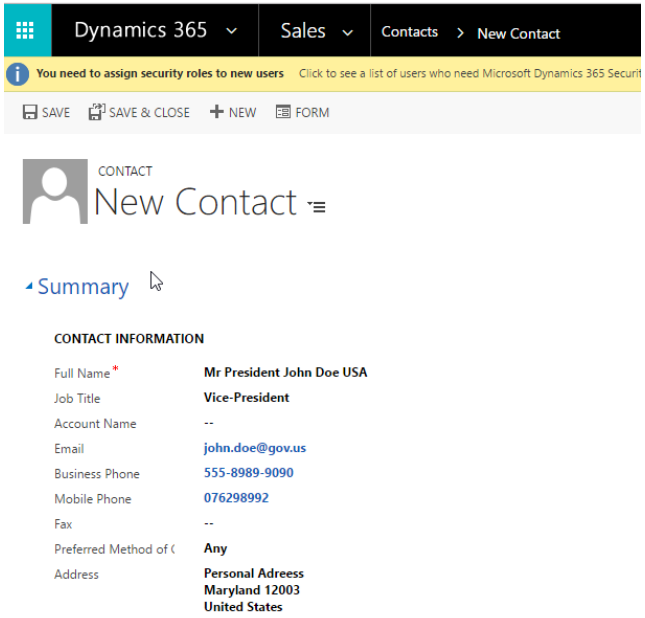
No wildcard nor boolean search

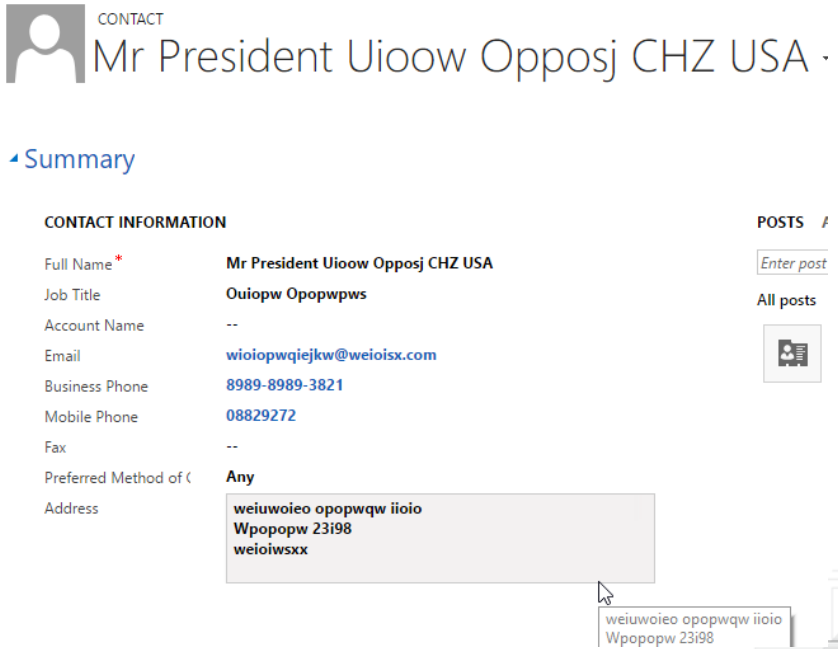
Case sensitive search

Sensible to known text attack and statistical attack

	Plaintext	Ciphertext
Document #1	And a good south wind sprung up behind; The Albatross did follow, And every day, for food or play, Came to the mariner's hollo!	B5E2 0020 7734 AFF3 C281 142F BB12 D99A 9987 4377 C3D2 8A8B 443E BB98 B5E2 4512 3BDF BB98 35A1 1A4F E210 D978 BB98 12FE 8228 **0D9E** F2B9 DF20 71AA
Document #2	And the good south wind still blew behind, But no sweet bird did follow, Nor any day for food or play Came to the mariner's hollo!	B5E2 **0D9E** 7734 AFF3 C281 72D0 1509 D99A BB98 CD40 000D 7851 12DE 8A8B 443E BB98 F33D 517D 3BDF 35A1 1A4F E210 D978 12FE 8228 **0D9E** F2B9 DF20 71AA

Format preserving encryptions





Format preserving encryptions

You cannot search directly through data encrypted with FPE

Lot of functionalities will break
    Search, Order by, Filtering, calculation ..
    Most of the server side features based on fields values

You cannot apply it to all kind of format and ensure the same level of security on all format

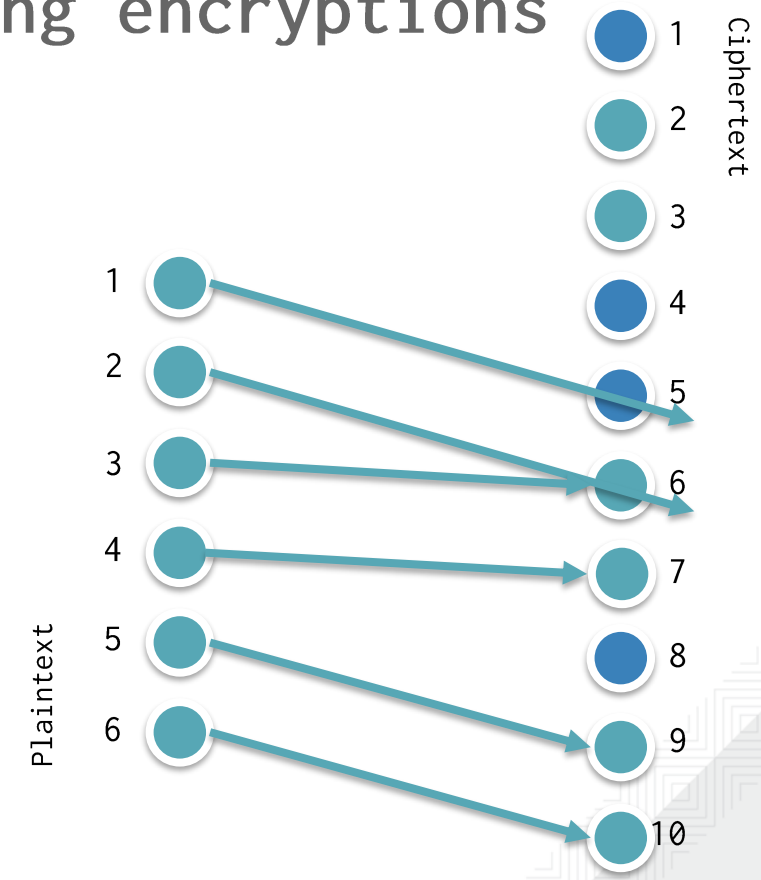
We released Go implementation of FPE available on :
https://github.com/cloudtrust/fpe

OPE Order preserving encryptions

You can order by

You can't apply content filter as "everything starting by 5"

Functionality based on content will break



Searchable encryption

Most of the paper imply a “build your own DB approach”

All approach will imply some leakage and limitations

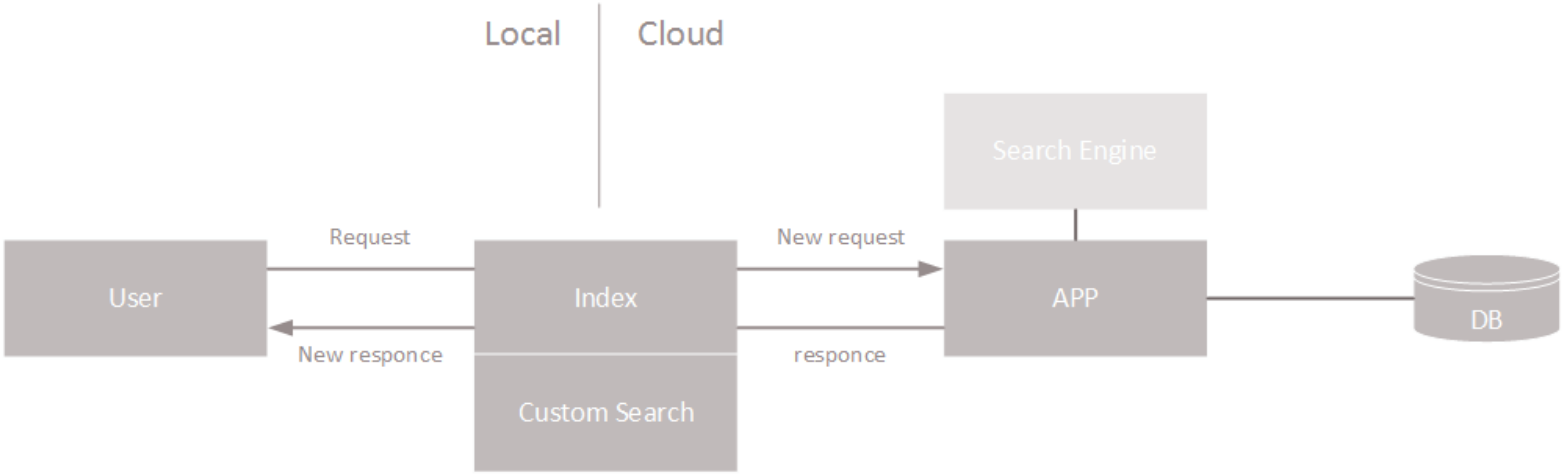
Index, special fields, ..

Current encrypted index approach imply to give-up the concept of high availability

Some approach as HVE impact dramatically performance

Searchable encryption

What tend to emerge



Have to re-create responce
You own dedicated DB / Index

Summary

Cloudtrust project is still at the beginning

We have a beta program to get information and opinion from our customers

We currently focus on the ACCESS part by extending keycloak with opensource addition

Searchable encryption require lot of tradeoff and still a moving target

Other project from ELCA are integrated within the cloudtrust approach

RED HAT FORUM

Europe, Middle East & Africa

Bonus

Design drivers

Share most of the platform and architecture between on-premise deployment and SaaS services

Allow to release same software with same tools

Keep OPEX stable

Help to define per users/capacity cost of operation

Allow technology migration over time

Avoid vendor locking, allow to keep framework updated and technology attractive & performant

Multi-tenancy

Required for multiple customers support

Design drivers

Horizontal scalability and Multi-DC support

Required on premise for high-availability, Required on SaaS to scale with customers growth

Reproducible & cost efficient

Avoid regression, smooth releases and day to day operations, reduce time to market, continuous delivery & tests

Use vanilla and standard technology stack

Allow easy and smooth migration from used technology, make upgrades a formality

Embark others ELCA Project

Multiple related security project

CloudTrust, MFA, Key management, …

Multiple related consulting opportunities

IAM projects, Federation Projects, User workflow projects

Internal collaboration

Others project, IAM and users management as a services (ELCA SAAS solution)

A global strategy is required

Regroup knowledge and improve design & architecture

Our plan regarding keycloak

We will create multiples operability modules to orchestrate keycloak at our will

We created a pet services to extend what keycloak can’t directly do

We created a partnership with redhat

We started adding new features to keycloak main codebase

We started introducing keycloak to other internal & External ELCA project

Keycloak integration