Secure your application with Artichokes

Casey Schaufler
Tomasz Świerczek

TIZEN™
DEVELOPER CONFERENCE
2014
SAN FRANCISCO

A word about our vegetable

- Artichoke in English
- Karczoch in Polish
- Cynara in Latin

The ones we didn’t use

- Polkit

- Polecat

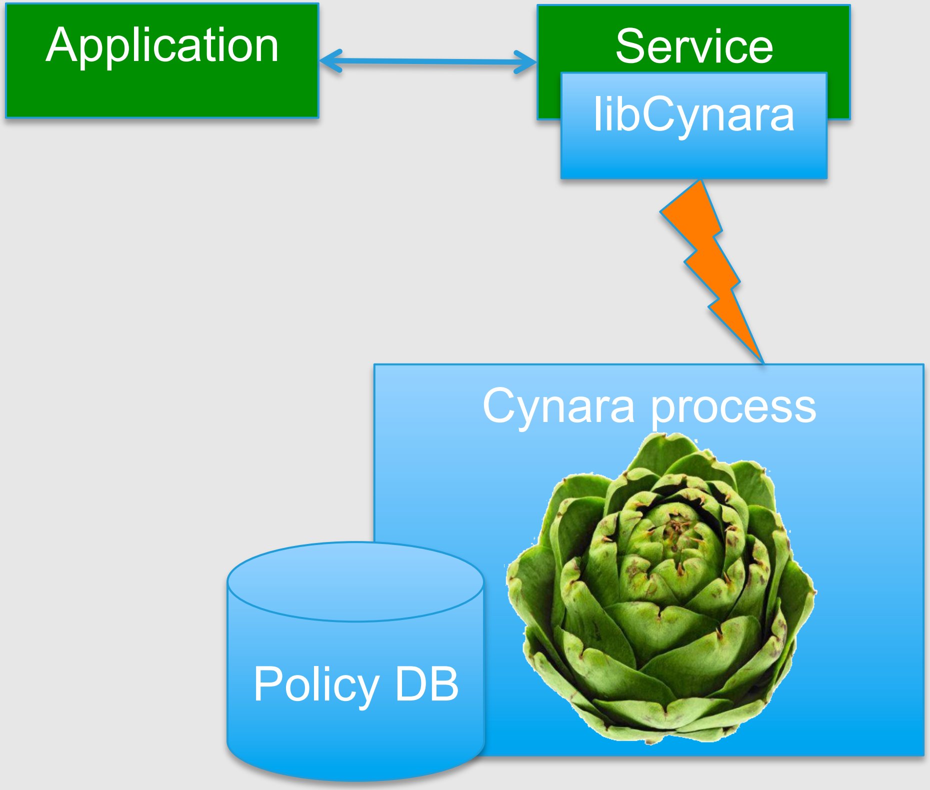
Polkit

What problem are we solving?

- Access control
- Arbitrary applications
- Abstract resources

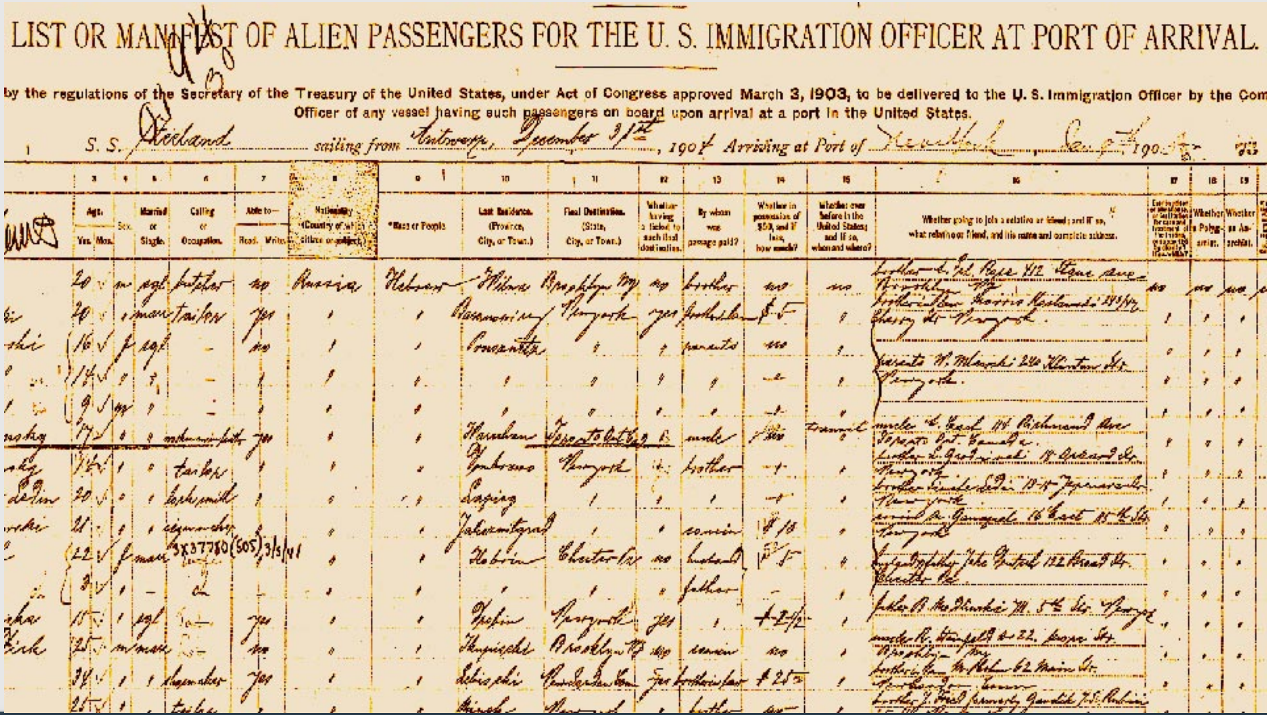
What is Cynara?

- A library
- A dedicated service
- A policy DB



What does the application have to do?

- Application manifest
- List of privileges
- Smack label assigned by the installer



LIST OR MANIFEST OF ALIEN PASSENGERS FOR THE U. S. IMMIGRATION OFFICER AT PORT OF ARRIVAL.

by the regulations of the Secretary of the Treasury of the United States, under Act of Congress approved March 3, 1903, to be delivered to the U. S. Immigration Officer by the Com
Officer of any vessel having such passengers on board upon arrival at a port in the United States.

S. S. Zeeland sailing from Antwerp, December 31st, 1904 Arriving at Port of New York Jan 9th 1905

	3		4	5	6	7		8	9	10	11	12	13	14	15	16	17	18	19
	Age.		Sex.	Married or Single.	Calling or Occupation.	Able to—		Nationality. (Country of which citizen or subject.)	*Race or People.	Last Residence. (Province, City, or Town.)	Final Destination. (State, City, or Town.)	Whether having a ticket to such final destination.	By whom was passage paid?	Whether in possession of $50, and if less, how much?	Whether ever before in the United States; and if so, when and where?	Whether going to join a relative or friend; and if so, what relative or friend, and his name and complete address.	[illegible]	Whether a Polygamist.	Whether an Anarchist.
	Yrs.	Mos.				Read.	Write.												
	20		m	sgl	butcher	no		Russia	Hebrew	Wilna	Brooklyn NY	no	brother	no	no	brother [illegible] Pope 412 Stone ave Brooklyn NY	no	no	no

What about run time?

- Nothing

- We don't trust applications

Credentials identify the application

- Smack label

What does the server have to do?

- Know its privileges

- Get credentials

- Call APIs

Cynara APIs

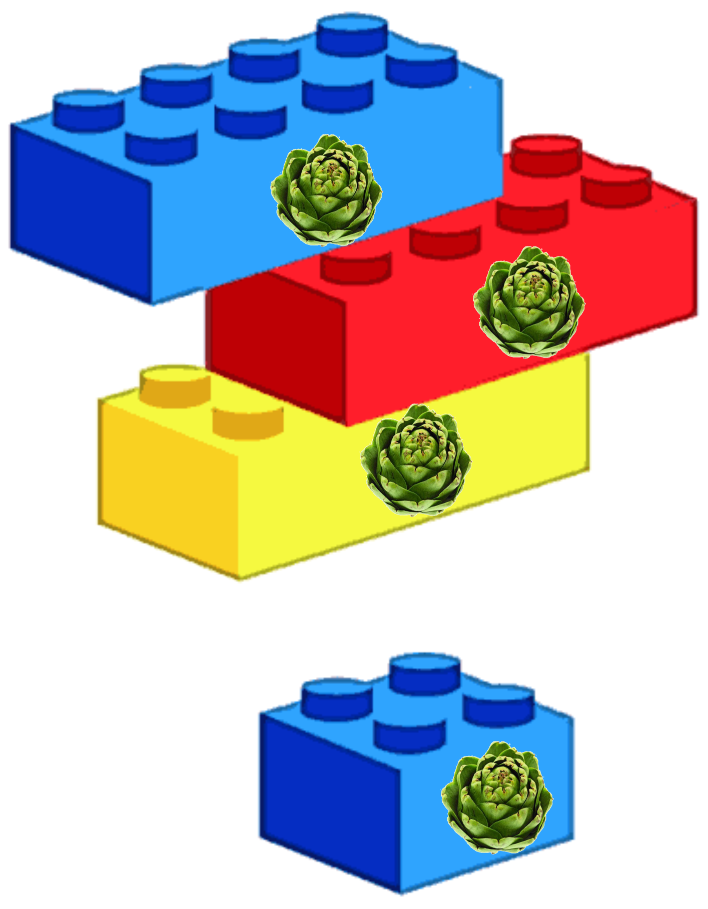
- **2 parts**
  - Checking privilege
  - Registering applications data
- **Synchronous API first**
  - Need for asynchronous agreed, will be provided later

Cynara APIs for services

- **Checking privilege – cynara-client**
  - **initialize()** & **finalize()**
    - Configurable: socket name, client cache size, …
  - **cynara_check()** with args:
    - Application id
    - Applications session id
    - User id
    - Privilege requested
  - Result: **SUCCESS** or **ACCESS_DENIED**

Cynara APIs for policy setup

- **cynara-admin library**
  - Registering applications privileges
  - Registering extensions to policy
    - possible UI popups



Cynara performance

- **Cynara good**
  - < 10 ms for Yes/No DB query
  - Can be optimized with client-side cache

- **Polkit bad**
  - > 30 ms for Yes/No DB query
  - Linear increase with # of rules
    - Javascript & XML policy DB

Cynara future directions

- **Current state – alpha working**
  - cynara-client library operational
  - No dedicated cynara service yet
- **Roadmap**
  - Dedicated process – **EOF June**
  - cynara-admin – **EOF June**
  - cynara-client cache – **EOF July**
  - Moving to github – **EOF July**
  - Async client API – **EOF August**
  - Extensions – **EOF August**

Thank you