Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Exercise Session 1

Introduction to the ACME Project

Elham Ehsani
Marc Wyss
Daniele Del Giudice

Obtaining a Certificate - The Classic Way

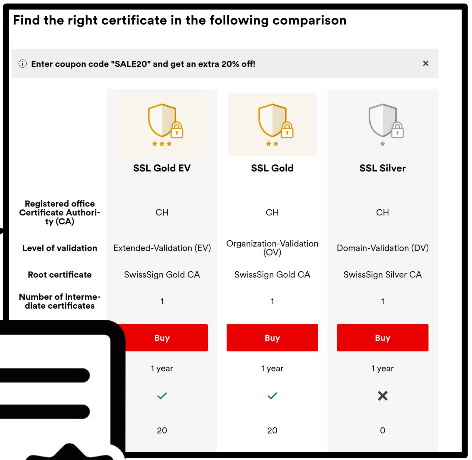
my-server.ch

Certificate Authority (CA)

Generate (K_{pub}, K_{priv})

Generate CSR for (my-server.ch, K_{pub})

Receive certificate at *webmaster@my-server.ch*

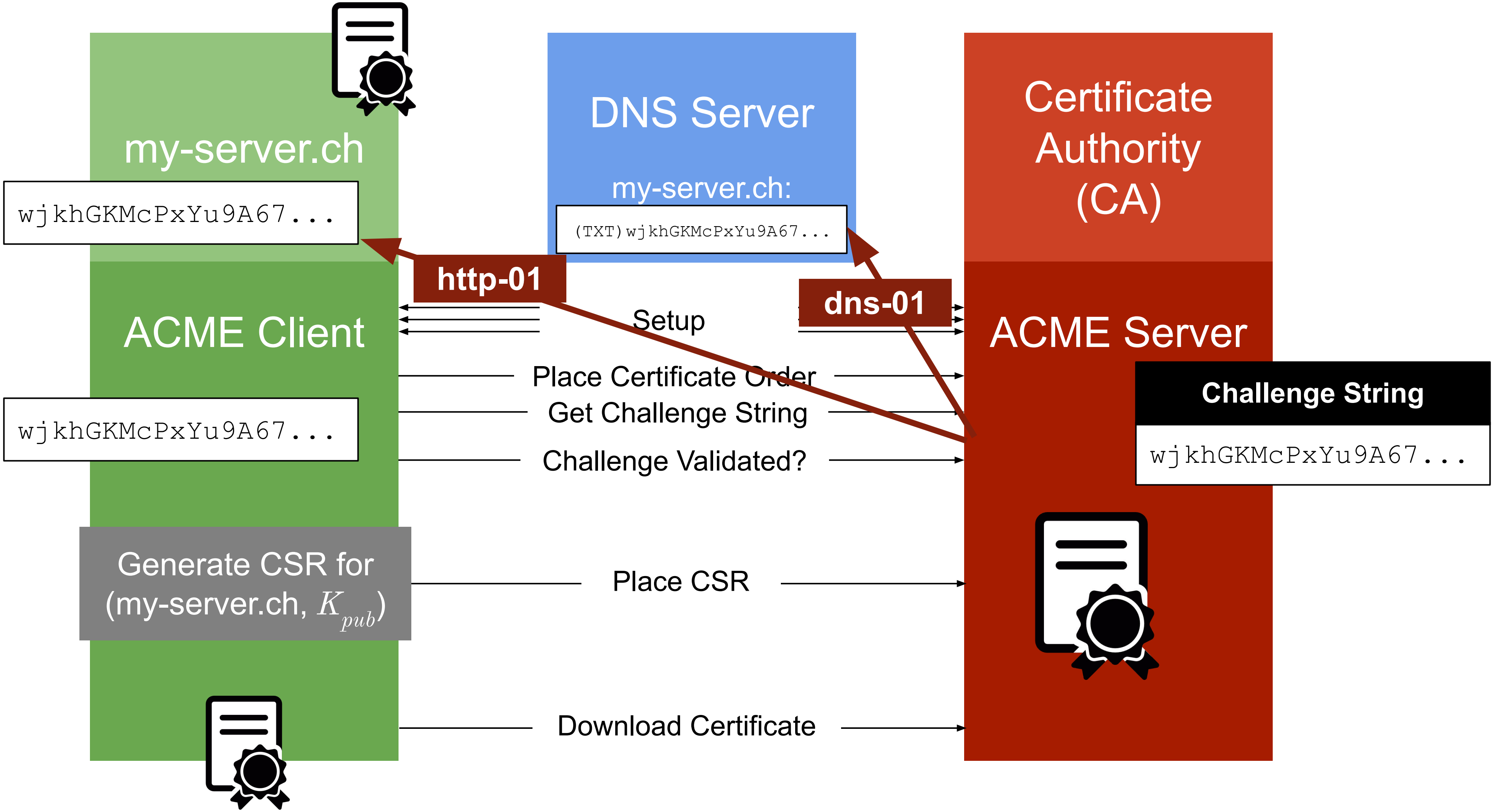


Find the right certificate in the following comparison

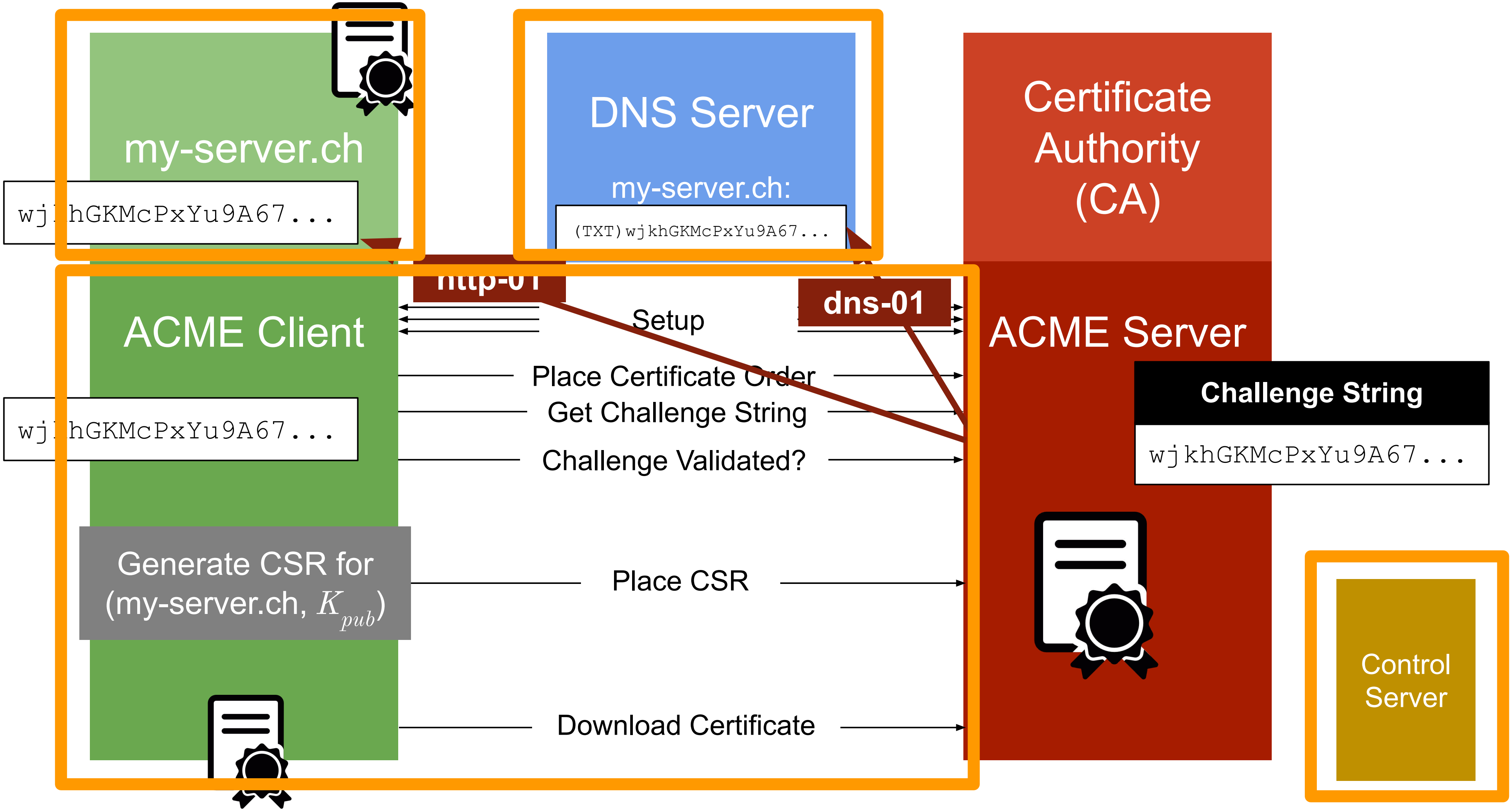
ⓘ Enter coupon code "SALE20" and get an extra 20% off! ×

	SSL Gold EV	SSL Gold	SSL Silver
Registered office Certificate Authority (CA)	CH	CH	CH
Level of validation	Extended-Validation (EV)	Organization-Validation (OV)	Domain-Validation (DV)
Root certificate	SwissSign Gold CA	SwissSign Gold CA	SwissSign Silver CA
Number of intermediate certificates	1	1	1
	Buy	Buy	Buy
	1 year	1 year	1 year
	✓	✓	✕
	20	20	0

Obtaining a Certificate - ACME (sketch)



What You Have to Implement in the Project



Information about the Project

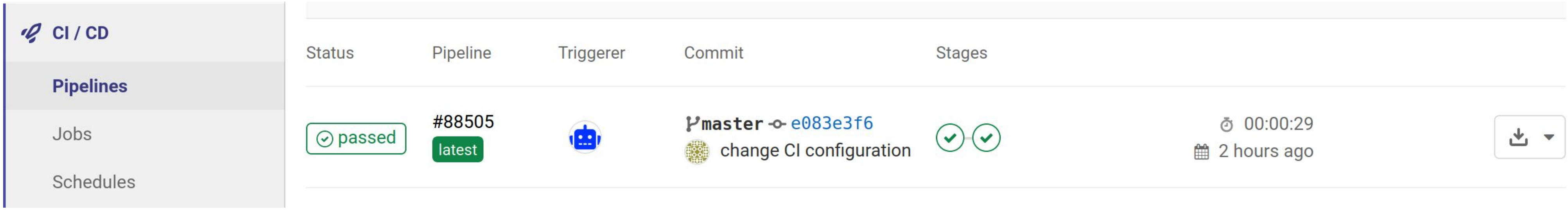
- Project description on gitlab.inf.ethz.ch at *NetSec 2023 Student Resources / projects*

- ACME is very well documented in RFC 8555.
  Reading and understanding a standard
  is a large part of this project.

- A repository with a code skeleton has been initialized for you on gitlab.inf.ethz.ch
    - If you registered for the course recently,
      there may not be a repository for you yet

Information about the Project

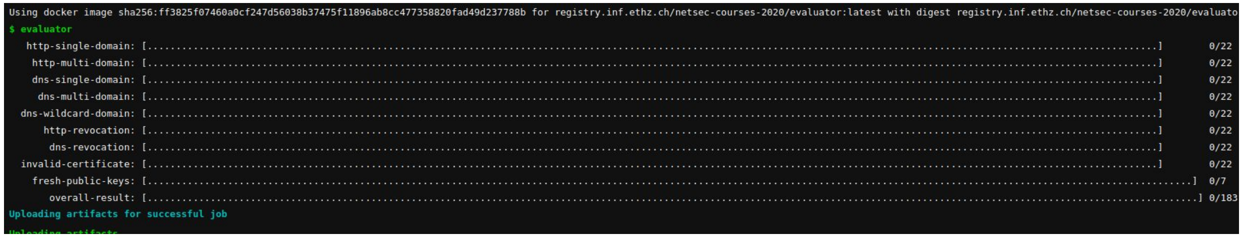
- Whenever you push to your repository,
  your code will be automatically tested by CI



Status	Pipeline	Triggerer	Commit	Stages		
passed	#88505 latest		master e083e3f6 change CI configuration	✓ ✓	00:00:29 2 hours ago	

- passed only means that the tests ran through,
  not that your implementation passed the tests!

Actual score
from output of job
give_score:



```
Using docker image sha256:ff3825f07460a0cf247d56038b37475f11896ab8cc477358820fad49d237788b for registry.inf.ethz.ch/netsec-courses-2020/evaluator:latest with digest registry.inf.ethz.ch/netsec-courses-2020/evaluato
$ evaluator
   http-single-domain: [........................................................................................................................................................................................................]        0/22
    http-multi-domain: [........................................................................................................................................................................................................]        0/22
    dns-single-domain: [........................................................................................................................................................................................................]        0/22
     dns-multi-domain: [........................................................................................................................................................................................................]        0/22
  dns-wildcard-domain: [........................................................................................................................................................................................................]        0/22
      http-revocation: [........................................................................................................................................................................................................]        0/22
       dns-revocation: [........................................................................................................................................................................................................]        0/22
  invalid-certificate: [........................................................................................................................................................................................................]        0/22
    fresh-public-keys: [...............................................................................................................................................................................................................]  0/7
       overall-result: [................................................................................................................................................................................................................] 0/183
Uploading artifacts for successful job
Uploading artifacts
```

Information about the Project

- Don’t use the Gitlab testing for debugging, as the computational resources are limited

- Better use **Pebble**, an ACME server implementation that you can run locally on your machine

- JOSE cryptography can be tricky, so plan enough time to implement it.

- Last submission before
  10 November 2023, 23:59
  determines grading.

Questions?

- If you have any questions during the project time, please read the ACME project FAQ first.
- If the FAQ do not contain your question, please use the Gitlab issues.