ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Exercise Session 1

Introduction to the ACME Project

Luca Tagliavini
Marc Wyss

Obtaining a Certificate - The Classic Way

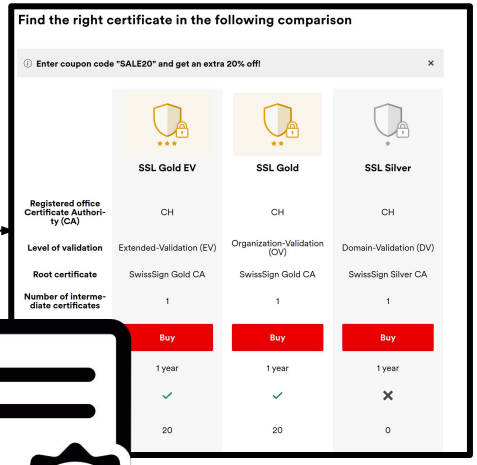
my-server.ch

Certificate Authority (CA)

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

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

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

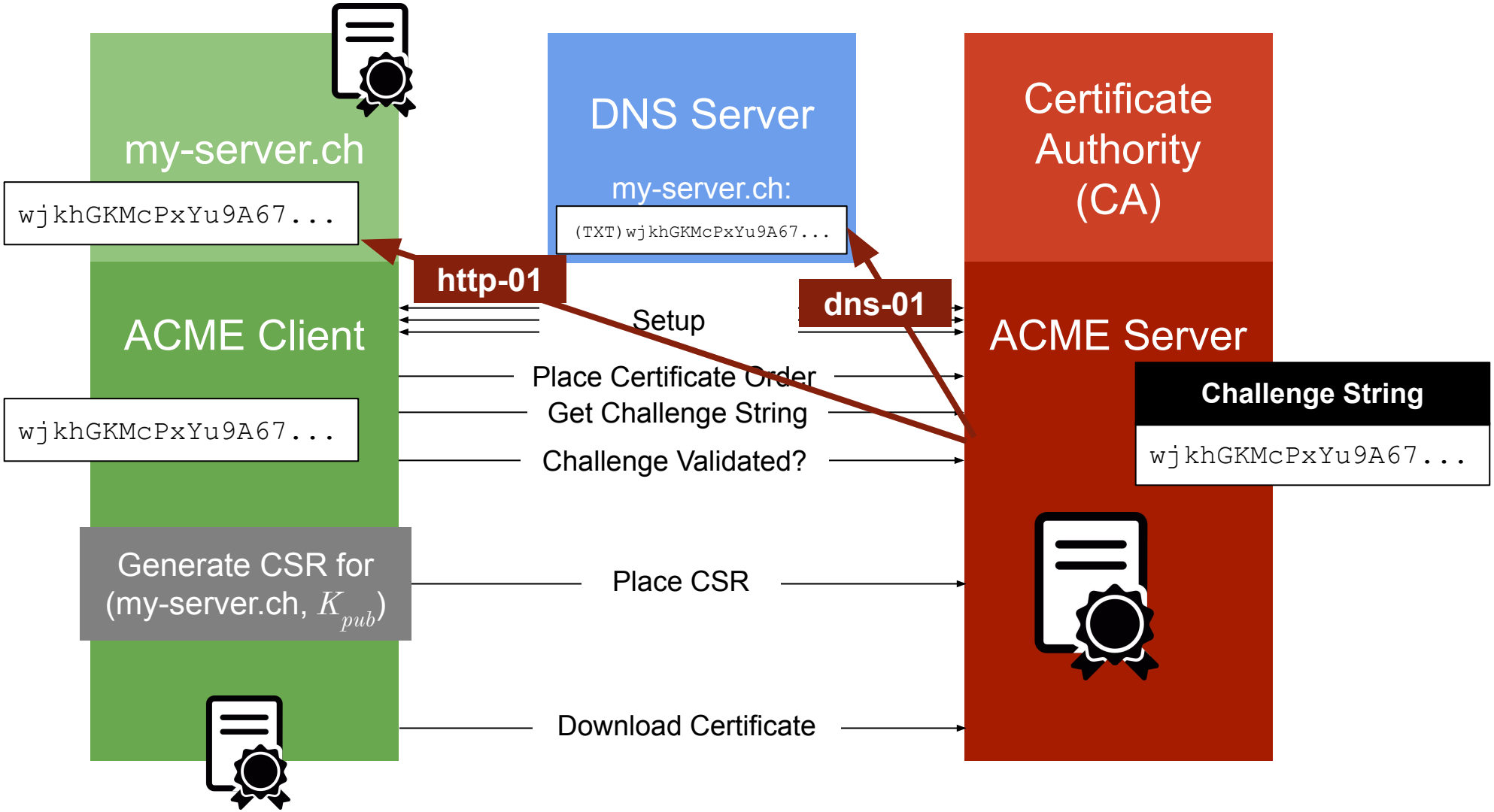


Find the right certificate in the following comparison

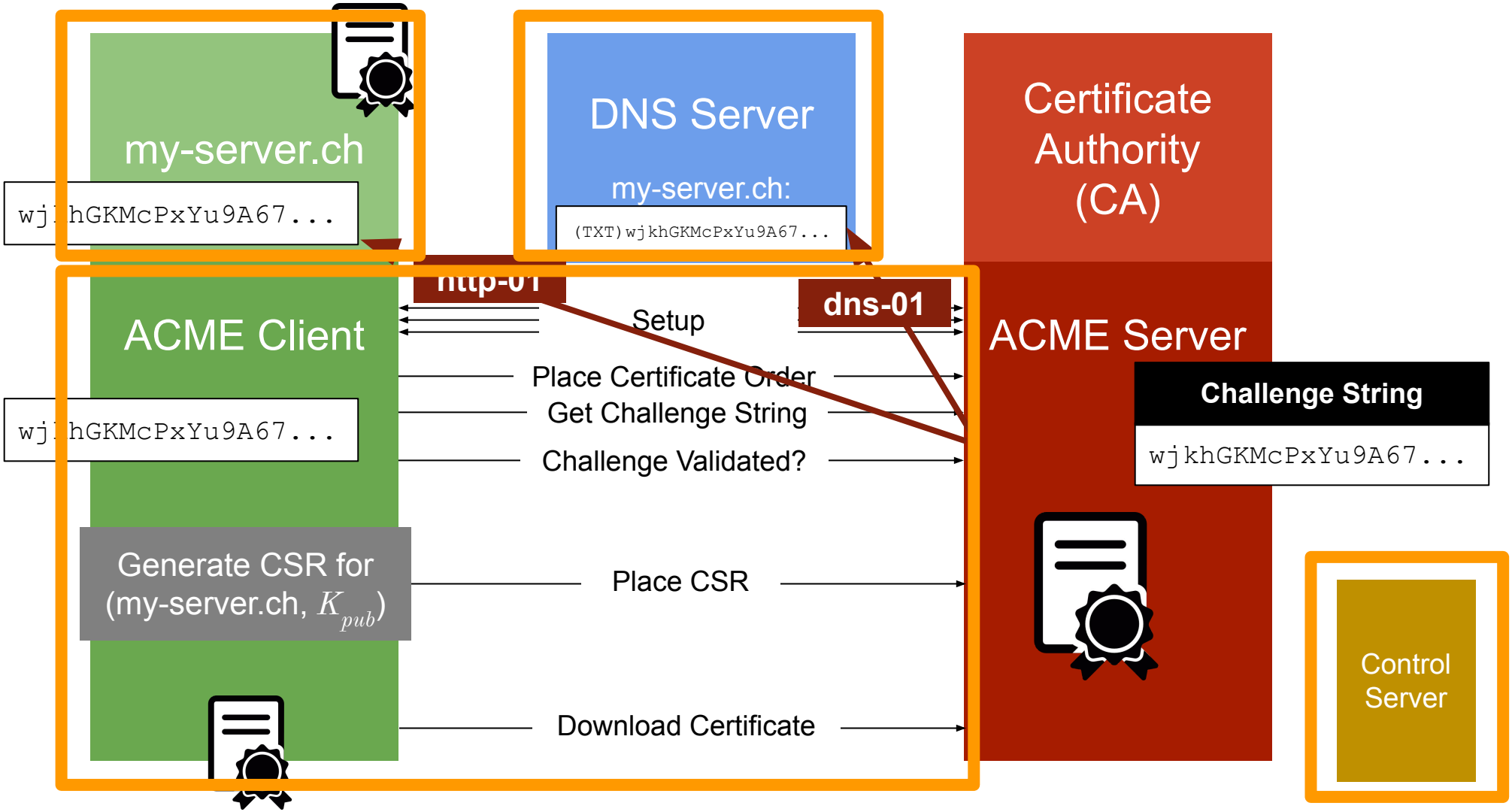
Enter coupon code "SALE20" and get an extra 20% off!

	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 2024 Student Resources / projects*

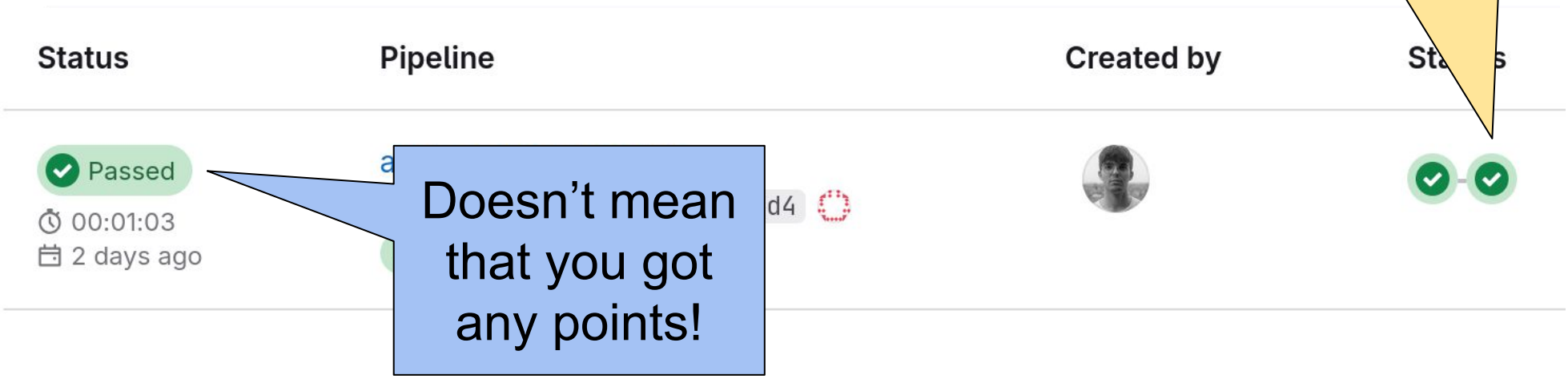
- ACME is very well documented in RFC 8555. Reading and understanding a standard is a large part of this project.

- A barebones repository has been initialized for you on gitlab.inf.ethz.ch
  - You **must copy** the template for your preferred language from Student Resources / projects / acme_templates
  - Be mindful of the library whitelist for each programming language

Project grading

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

You need to check the output



Doesn't mean that you got any points!

- The jobs will fail until a template is applied.

Project grading - continued

```
$ evaluator
  http-single-domain: [==========================================================================================================]        22/22
   http-multi-domain: [==========================================================================================================]        22/22
   dns-single-domain: [==========================================================================================================]        22/22
    dns-multi-domain: [==========================================================================================================]        22/22
 dns-wildcard-domain: [==========================================================================================================]        22/22
     http-revocation: [==========================================================================================================]        22/22
      dns-revocation: [==========================================================================================================]        22/22
 invalid-certificate: [==========================================================================================================]        22/22
   fresh-public-keys: [==========================================================================================================]  7/7
       overall-result: [==========================================================================================================] 183/183
```

7 Functionality tests

+

2 Correctness Checks

=

Total of 183 points

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 **8 November 2024, 23:59** determines grading.

You can find hints in the FAQ

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.