

**This presentation is more than one year old.  
Some parts may be outdated.**

You can find the latest information here:

**<https://www.frogans.org/en/main.html>**

## Purpose of the addressing system of a medium for publishing content on the Internet

- from a human point of view: the system has to enable end users to confirm access to a given content using a visible identifier (a string of characters)
- from a technical point of view: the system has to provide the client with the technical characteristics of the connection to be established with the server (e.g. protocols)

## World Wide Web

In the addressing system for Web pages, human and technical matters are **merged**.

The visible identifier is a URL which contains the technical characteristics of the connection:

```
https://www.specificdomainname.com/directoriest/document-name.extension
```

While being easy to implement, this addressing system presents two problems:

- End users are exposed to technical information that most of them can't understand.
- The technical characteristics are insufficiently detailed<sup>1</sup>. For instance, security characteristics are reduced to a single character (the s in "https").

<sup>1</sup> This is because otherwise URLs would become impractical for humans and URL-based links would break whenever a technical characteristic is changed.

## Frogans

In the addressing system for Frogans sites, human and technical matters are **separated**.

1) The visible identifier is a Frogans address<sup>1</sup>:

```
network-name*site-name
```

2) The technical characteristics of the connection are not visible to end users.

They are defined using a UCSR<sup>2</sup> path, which is an exhaustive set of technical parameters represented by an XML element<sup>3</sup>.

The UCSR path is defined and updated by the Frogans site publisher<sup>4</sup>. It is retrieved when the Frogans address is resolved on the Internet<sup>5</sup>.

<sup>1</sup> Described in the IFAP and FACR specifications

<sup>2</sup> Uniform Content Server Request

<sup>3</sup> Described in the UCSR specifications

<sup>4</sup> Described in the FCR-MSI specification

<sup>5</sup> Described in the FNSL specification

## Example of a UCSR path for the UCSR network **IP\_DNS\_TCP\_HTTP**

```
<ucsr-path network='IP_DNS_TCP_HTTP'>
  <location>public</location>
  <domain-name>www.specificdomainname.com</domain-name>
  <port>80</port>
  <directory>/public/demo/helloworld</directory>
</ucsr-path>
```

## Example of a UCSR path for the UCSR network **IP\_DNS\_TCP\_TLS\_HTTP**

```
<ucsr-path network='IP_DNS_TCP_TLS_HTTP'>
  <location>public</location>
  <domain-name>www.specificdomainname.com</domain-name>
  <port>443</port>
  <tls-version>1.2</tls-version>
  <certificate-rollover-ongoing>no</certificate-rollover-ongoing>
  <current-ciphersuite>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</current-ciphersuite>
  <current-exchange-elliptic-curve>prime256v1</current-exchange-elliptic-curve>
  <current-certificate-fingerprint>
    35ff28a0006a50ec8d3dc060d88960d2dabc23d0cf225026c0d5df4e3bbd1df3
    2525698c43786a37dfbbbaad9c96ca6f232125b4d042ba4864bb86c8770f07a1
  </current-certificate-fingerprint>
  <current-certificate-type>rsa</current-certificate-type>
  <current-certificate-rsa-key-size>4096</current-certificate-rsa-key-size>
  <directory>/public/demo/helloworld</directory>
</ucsr-path>
```

TLS characteristics  
used by the client  
for the connection  
to the server  
(define the  
security level for  
the connection)