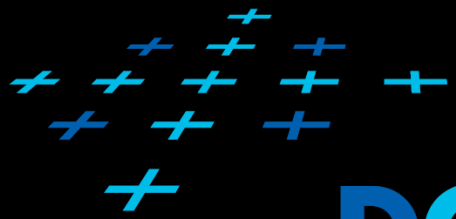


DCGI

KATEDRA POČÍTAČOVÉ GRAFIKY A INTERAKCE

Autentizace

Autentizace a Autorizace

- Autentizace
  - Znám Tvojí identitu
  - Obvykle se ověřuje pomocí jména a hesla, biometricky, apod.

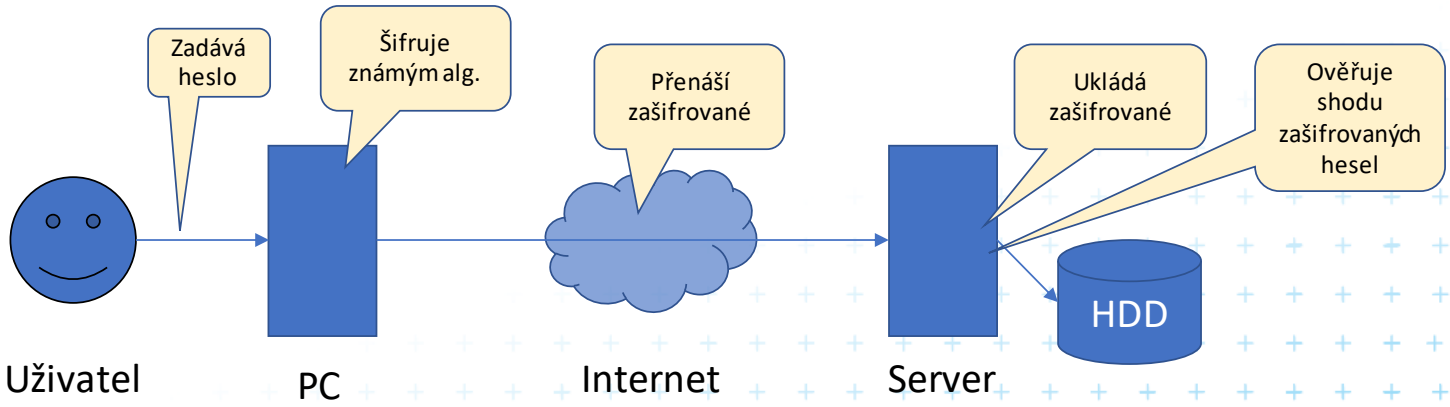
- Autorizace
  - Vím kdo jsi a řeším co smíš dělat
  - Obvykle systém oprávnění, skupiny, jednotlivci, role

Ukládání hesla

- Obecný problém
- Uživatel: jméno a heslo zná, pamatuje si ho
  - !!! nikam si ho nepíše, má ho v hlavě
- Server: jméno a heslo zná, jak si ho zapamatuje?
  - …někam si ho přeci zapsat musí
  - nikdy si heslo neukládá v přímé podobě, ukládá si jen jeho otisk - hash
- Solení hesla
  - hash hesla je zapsán na disk. Aby nešlo poznat, že dva uživatelé mají stejné heslo (stejný hash), přidává se před hashovaním známá jednoznačná „sůl“. Sůl je pro každého uživatele jiná, ale známá.

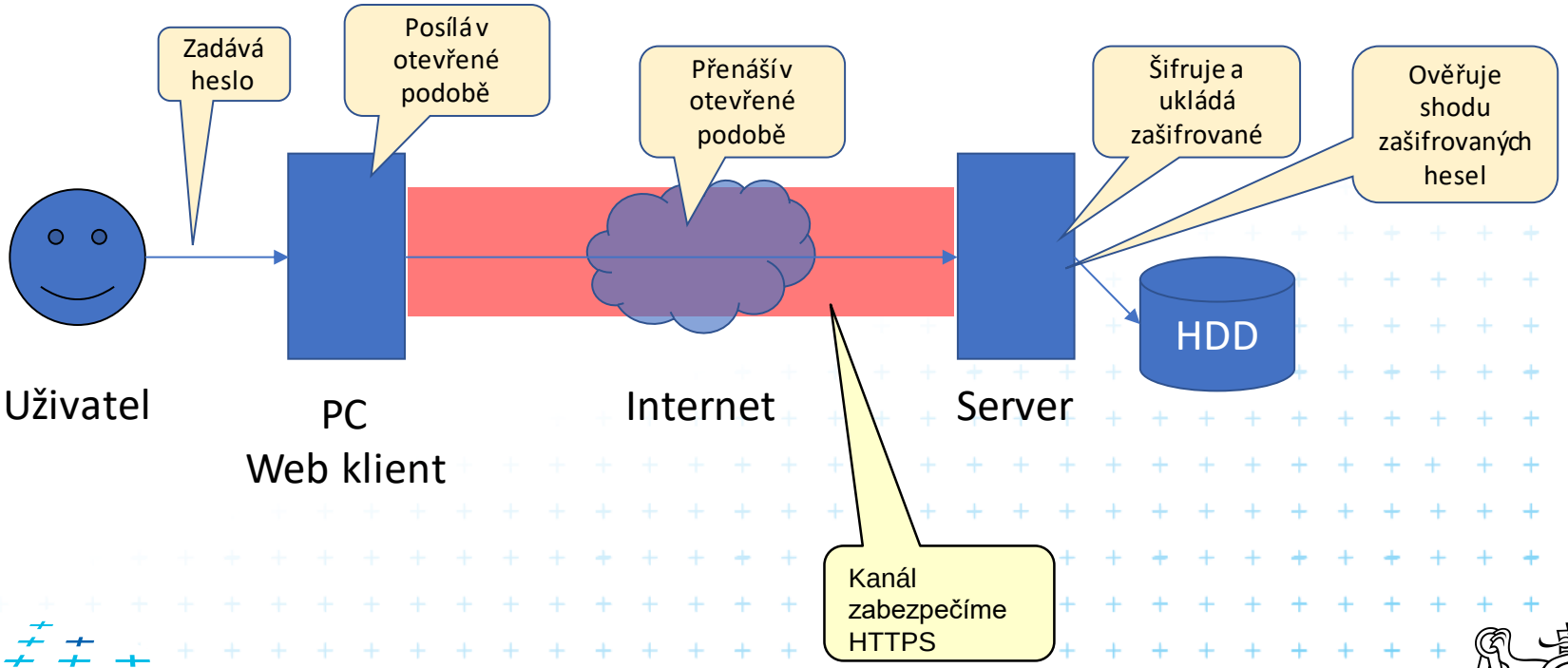
Ideální řešení

- Heslo nikdy neputuje přes internet v otevřené podobě
  - útok na přenos není efektivní
- Server heslo nezná, zná jenom jeho otisk
  - útok na server není efektivní



Webové obvyklé řešení

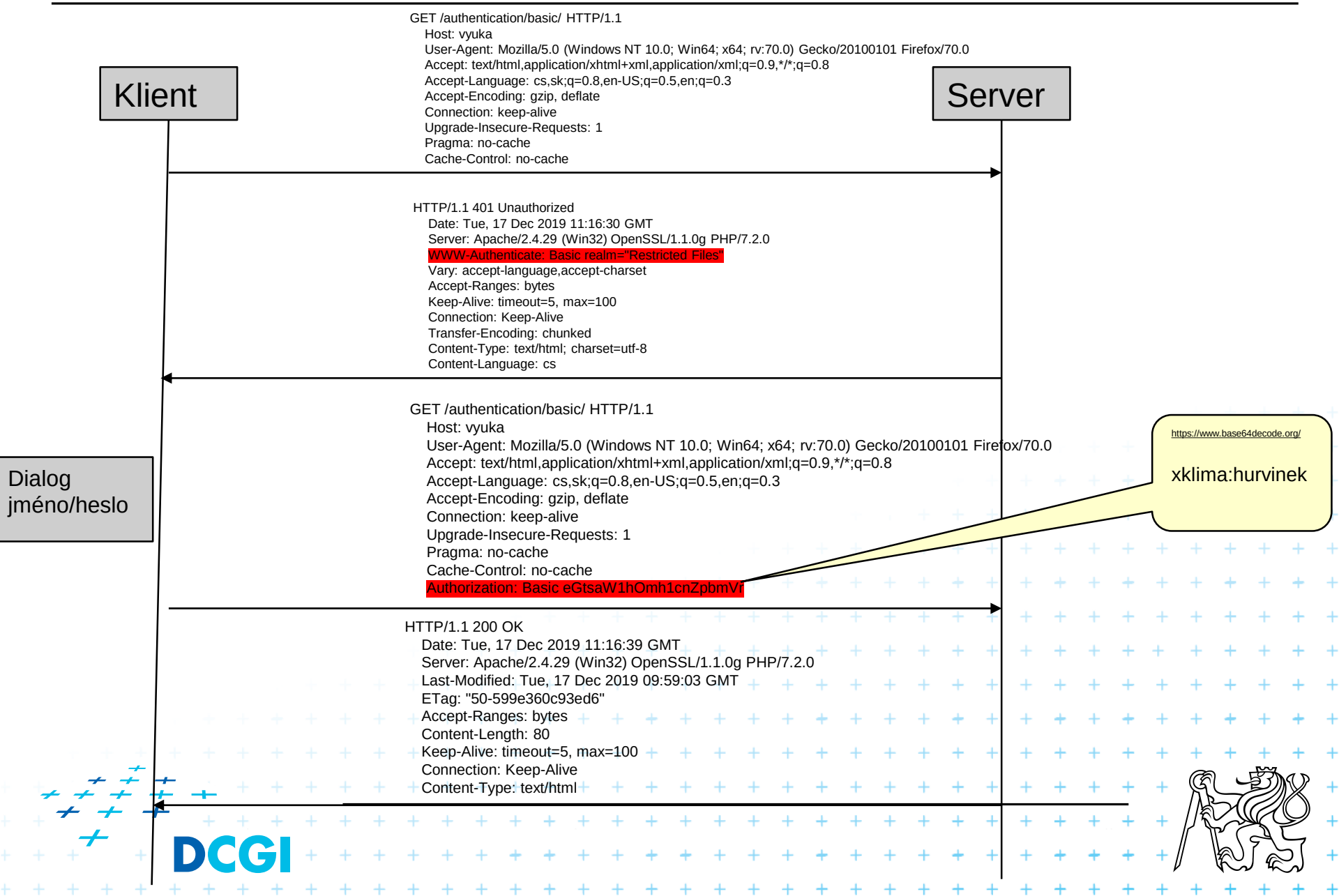
- Webový klient je „tenký“ a neumí šifrovat



Autentizace přímo v HTTP protokolu

- Dva základní druhy
  - Basic
  - Digest
- Basic
  - Nešifruje jméno a heslo
  - Přenos je pomocí kódování Base64 - https://www.base64encode.org/
- Digest
  - Šifruje jméno a heslo
- Oba typy ukládají heslo na serveru v ***šifrované*** podobě

HTTP Basic



DCGI

Basic - nastavení Apache mod_auth

.htaccess

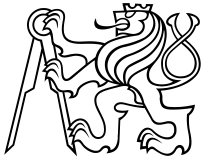
```
AuthType Basic
AuthName "Restricted Files"
# (Following line optional)
AuthBasicProvider file
AuthUserFile c:\www\vyuka\autentication\basic\.passwd
require valid-user
```

.password

```
xklima:$apr1$l9sbbAjg$ruUy6FCr0urJfjSvlEHsF/
vomacka:$apr1$7Fie0hsh$2YCOrY.CJndtLWNGwQOyG.
```

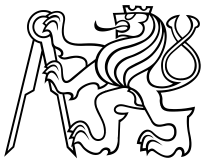
Přídání hesla

```
htpasswd.exe -c c:\www\vyuka\autentication\basic\.password xklima
```



Implementace v PHP

```php
<?php
if (
isset($_SERVER['PHP_AUTH_USER']) &&
isset($_SERVER['PHP_AUTH_PW']) &&
$_SERVER['PHP_AUTH_USER'] == 'uzivatel' &&
$_SERVER['PHP_AUTH_PW'] == '1234') { /* vse v poradku */
    echo 'Prihlaseni probehlo uspesne.';
}
else { /* chyba prihlaseni */
    header('HTTP/1.0 401 Unauthorized');
    header('WWW-Authenticate: Basic realm="Login"');
    echo 'Chyba prihlaseni - zadejte platne uzivatelske jmeno a heslo!';
    exit;
}
?>
```

Problémy

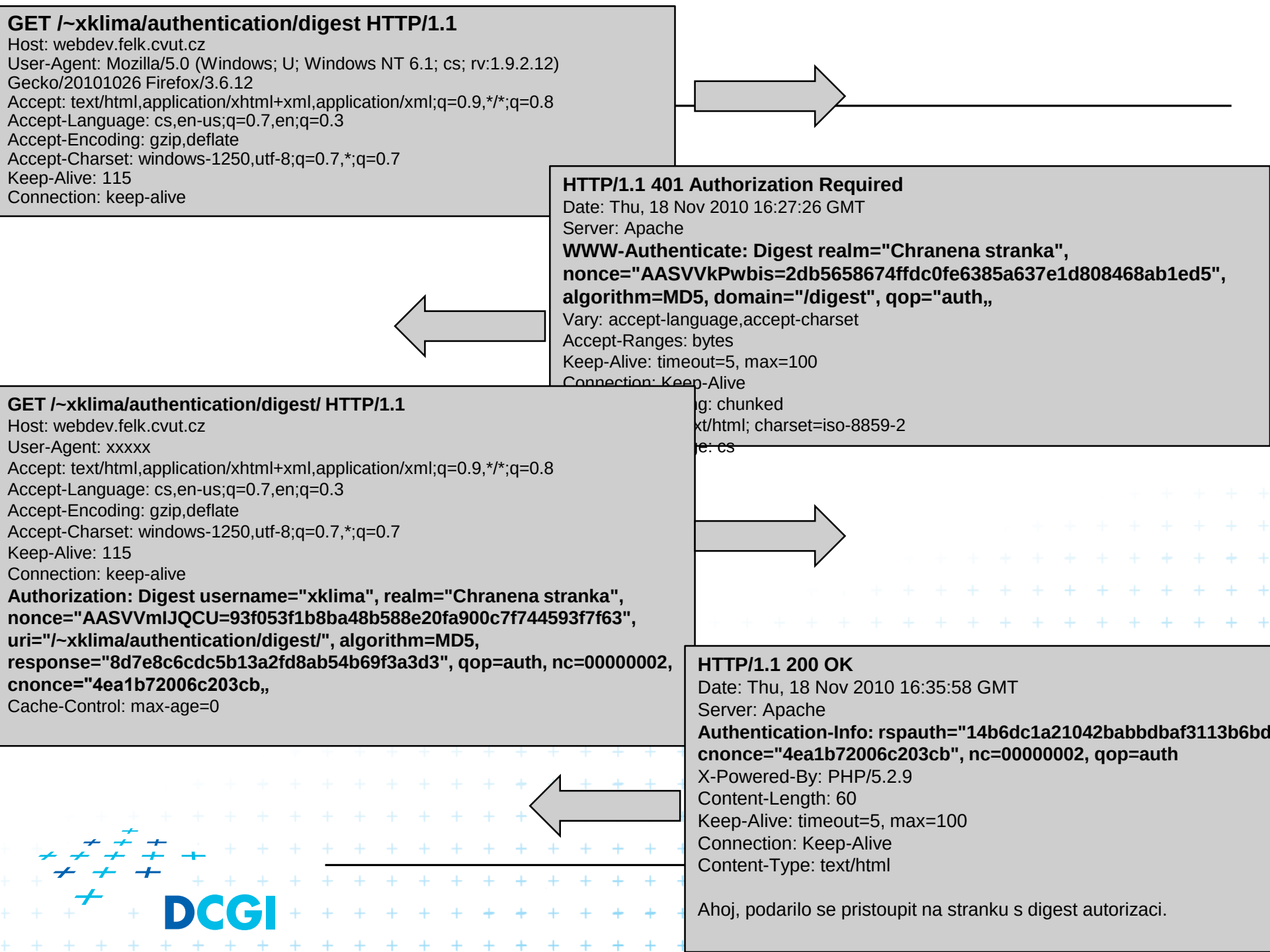
- Donutit klienta odhlásit se
  - klient si pamatuje přihlašovací string
- Zabezpečení hesla
  - je nutné zabezpečit kanál

Authorization: Digest

- Řeší problém posílání otevřených hesel
- Není podporováno všemi klienty

- Podmínky:
  - mod_digest

- Princip:
- založeno na hash MD5


GET /~xklima/authentication/digest HTTP/1.1
Host: webdev.felk.cvut.cz
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; cs; rv:1.9.2.12)
Gecko/20101026 Firefox/3.6.12
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: cs,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: windows-1250,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
HTTP/1.1 401 Authorization Required
Date: Thu, 18 Nov 2010 16:27:26 GMT
Server: Apache
WWW-Authenticate: Digest realm="Chranena stranka",
nonce="AASVVkPwbis=2db5658674ffdc0fe6385a637e1d808468ab1ed5",
algorithm=MD5, domain="/digest", qop="auth„
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
g: chunked
xt/html; charset=iso-8859-2
e: cs
GET /~xklima/authentication/digest/ HTTP/1.1
Host: webdev.felk.cvut.cz
User-Agent: xxxxx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: cs,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: windows-1250,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Authorization: Digest username="xklima", realm="Chranena stranka",
nonce="AASVVmIJQCU=93f053f1b8ba48b588e20fa900c7f744593f7f63",
uri="/~xklima/authentication/digest/", algorithm=MD5,
response="8d7e8c6cdc5b13a2fd8ab54b69f3a3d3", qop=auth, nc=00000002,
cnonce="4ea1b72006c203cb„
Cache-Control: max-age=0
HTTP/1.1 200 OK
Date: Thu, 18 Nov 2010 16:35:58 GMT
Server: Apache
Authentication-Info: rspauth="14b6dc1a21042babbdbaf3113b6bd
cnonce="4ea1b72006c203cb", nc=00000002, qop=auth
X-Powered-By: PHP/5.2.9
Content-Length: 60
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Ahoj, podarilo se pristoupit na stranku s digest autorizaci.
DCGI

Digest

.htaccess

```
AuthUserFile
c:\www_root\vyuka\autentizace\digest\hesla
AuthType Digest
AuthName "Chranena stranka"
AuthDigestDomain /digest
AuthDigestNonceLifetime 300
require valid-user
```

Zřízení souboru se jménem a heslem

```
htdigest -c c:\www_root\vyuka\autentizace\digest\hesla "Chranena stranka"
xklima
Adding password for xklima in realm Chranena stranka.
New password: ******
Re-type new password: ******
```

Soubor hesla

```
xklima:Chranena stranka:73fa9ff52b5a8f464303a68bb7a2e54f
```


Posílání citlivé informace přes síť

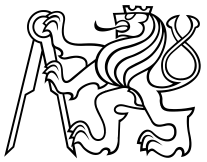
$$HA1 = MD5\Big(A1\Big) = MD5\Big(username : realm : password\Big)$$

$$HA2 = MD5\Big(A2\Big) = MD5\Big(method : digestURI\Big)$$

$$response = MD5\Big(HA1 : nonce : HA2\Big)$$

Další varianty

$$response = MD5\Big(HA1 : nonce : nonceCount : clientNonce : qop : HA2\Big)$$



Digest v PHP

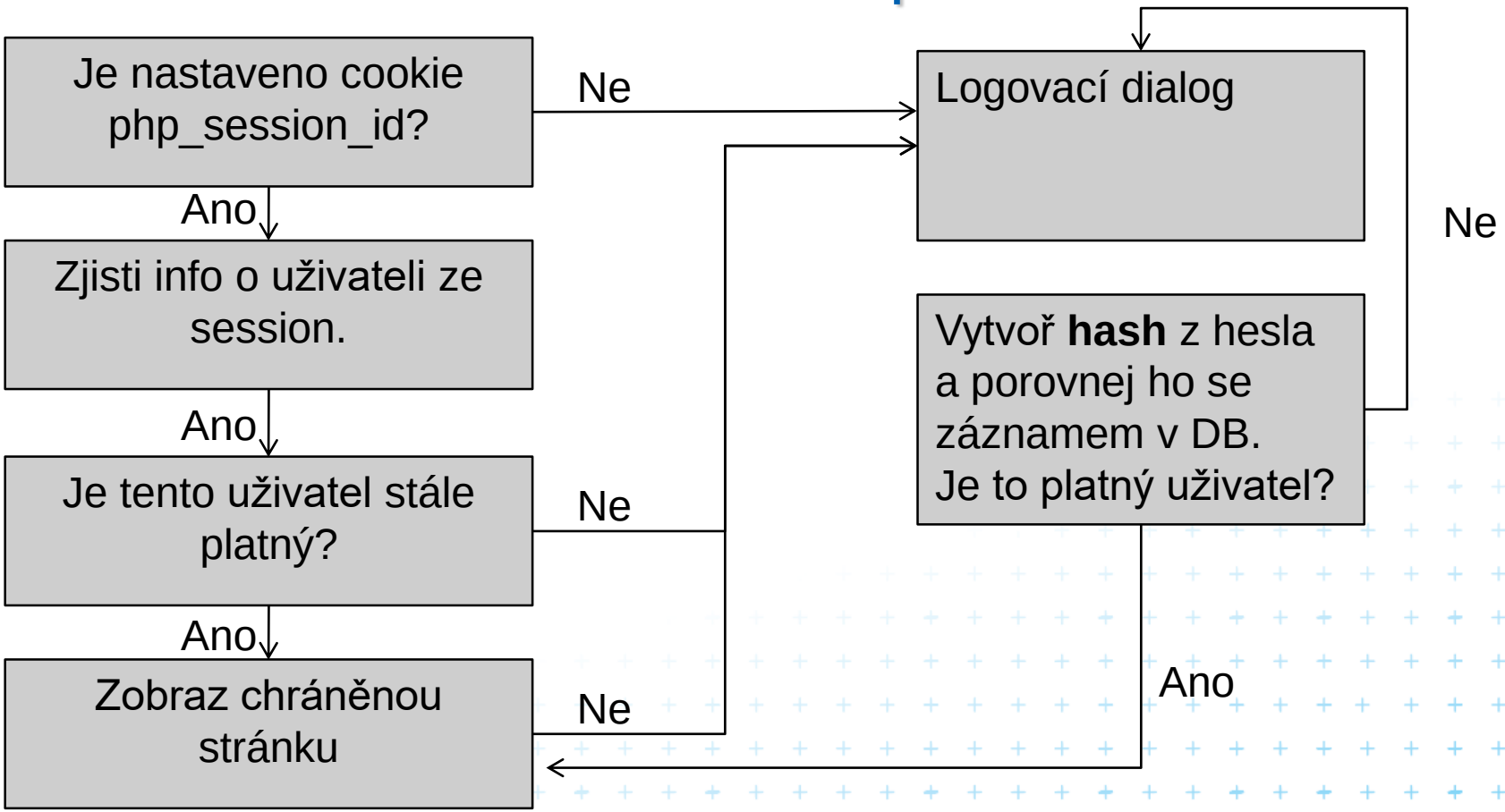
```php
$realm = 'Restricted area';
//user => password
$users = array('xklima' => 'martin', 'guest' => 'guest');

if (empty($_SERVER['PHP_AUTH_DIGEST'])) {
    header('HTTP/1.1 401 Unauthorized');
    header('WWW-Authenticate: Digest realm="'.$realm.
           '",qop="auth",nonce="'.uniqid().'",opaque="'.md5($realm).'"');

    die('Text to send if user hits Cancel button');
}

// analyze the PHP_AUTH_DIGEST variable
if (!($data = http_digest_parse($_SERVER['PHP_AUTH_DIGEST'])) ||
    !isset($users[$data['username']]))
    die('Wrong Credentials!');

// generate the valid response
$A1 = md5($data['username'] . ':' . $realm . ':' . $users[$data['username']]);
$A2 = md5($_SERVER['REQUEST_METHOD'].':'.$data['uri']);
$valid_response = md5($A1.':'.$data['nonce'].':'.$data['nc'].':'.$data['cnonce'].':'.$data['qop'].':'.$A2);

if ($data['response'] != $valid_response)
    die('Wrong Credentials!');

// ok, valid username & password
echo 'Your are logged in as: ' . $data['username'];

?>
```

Digest v PHP

```php
// function to parse the http auth header
function http_digest_parse($txt)
{
    // protect against missing data
    $needed_parts = array('nonce'=>1, 'nc'=>1, 'cnonce'=>1, 'qop'=>1, 'username'=>1, 'uri'=>1, 'response'=>1);
    $data = array();
    $keys = implode('|', array_keys($needed_parts));

    preg_match_all('@(' . $keys . ')=(?:([\'"])([^\2]+?)\2|([^\s,]+))@', $txt, $matches, PREG_SET_ORDER);

    foreach ($matches as $m) {
        $data[$m[1]] = $m[3] ? $m[3] : $m[4];
        unset($needed_parts[$m[1]]);
    }

    return $needed_parts ? false : $data;
}
```

Autentizace pomocí cookies, resp. session

- Řešíme to na úrovni PHP skriptu



Single Sign On (SSO)

- OAuth protokol