

DCGI

KATEDRA POČÍTAČOVÉ GRAFIKY A INTERAKCE

Autentikace



mod_auth

.htaccess

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

.password

```
xklima:$apr1$I9sbbAjb$ruUy6FCr0urJfjSvIEHsF/
vomacka:$apr1$7Fie0hsh$2YCOyY.CJndtLWNGwQOyG.
```

Přidání hesla

```
htpasswd.exe -c c:\www_root\vyuka\autentizace\apache\.password xklima
```

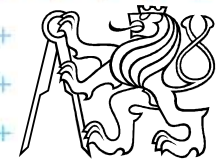


```
<?php
if (
isset($_SERVER['PHP_AUTH_USER']) &&
isset($_SERVER['PHP_AUTH_PW']) &&
$_SERVER['PHP_AUTH_USER'] == 'uzivatel' &&
$_SERVER['PHP_AUTH_PW'] == '1234') { /* vse v poradku */
    echo 'Prihlaseni probehlo uspesne.';
}
else { /* chyba prihlaseni */
    header('HTTP/1.0 401 Unauthorized');
 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



Problémy

- Donutit klienta odhlásit se
- Zabezpečení hesla



Authorization: Digest

- Řeší problém posílání otevřených hesel
- Není podporováno všemi klienty

- Podmínky:
 - mod_digest

- Princip:
- založeno na hash MD5



Digest

.htaccess

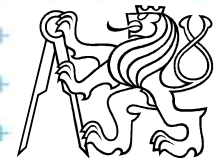
```
AuthUserFile  
c:\www_root\vyuka\autentizace\digest\hesla  
AuthType Digest  
AuthName "Chranena stranka"  
AuthDigestDomain /digest  
AuthDigestNonceLifetime 300  
require valid-user
```

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

$$HA1 = MD5(A1) = MD5(\text{username} : \text{realm} : \text{password})$$

$$HA2 = MD5(A2) = MD5(\text{method} : \text{digestURI})$$

$$\text{response} = MD5(HA1 : \text{nonce} : HA2)$$

Další varianty

$$\text{response} = MD5(HA1 : \text{nonce} : \text{nonceCount} : \text{clientNonce} : \text{qop} : HA2)$$



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

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="AASVvmlJQCU=93f053f1b8ba48b588e20fa900c7f744593f7f63",
uri="/~xklima/authentication/digest/", algorithm=MD5,
response="8d7e8c6cdc5b13a2fd8ab54b69f3a3d3", qop=auth, nc=00000002,
cnonce="4ea1b72006c203cb,,**
Cache-Control: max-age=0

g: chunked
t/html; charset=iso-8859-2
e: cs

HTTP/1.1 200 OK

Date: Thu, 18 Nov 2010 16:35:58 GMT
Server: Apache
**Authentication-Info: rspauth="14b6dc1a21042babdbaf3113b6bd
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.



Digest v 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'];

?>
```

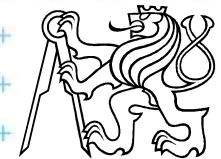
Digest v PHP

```
// 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);

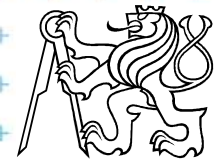
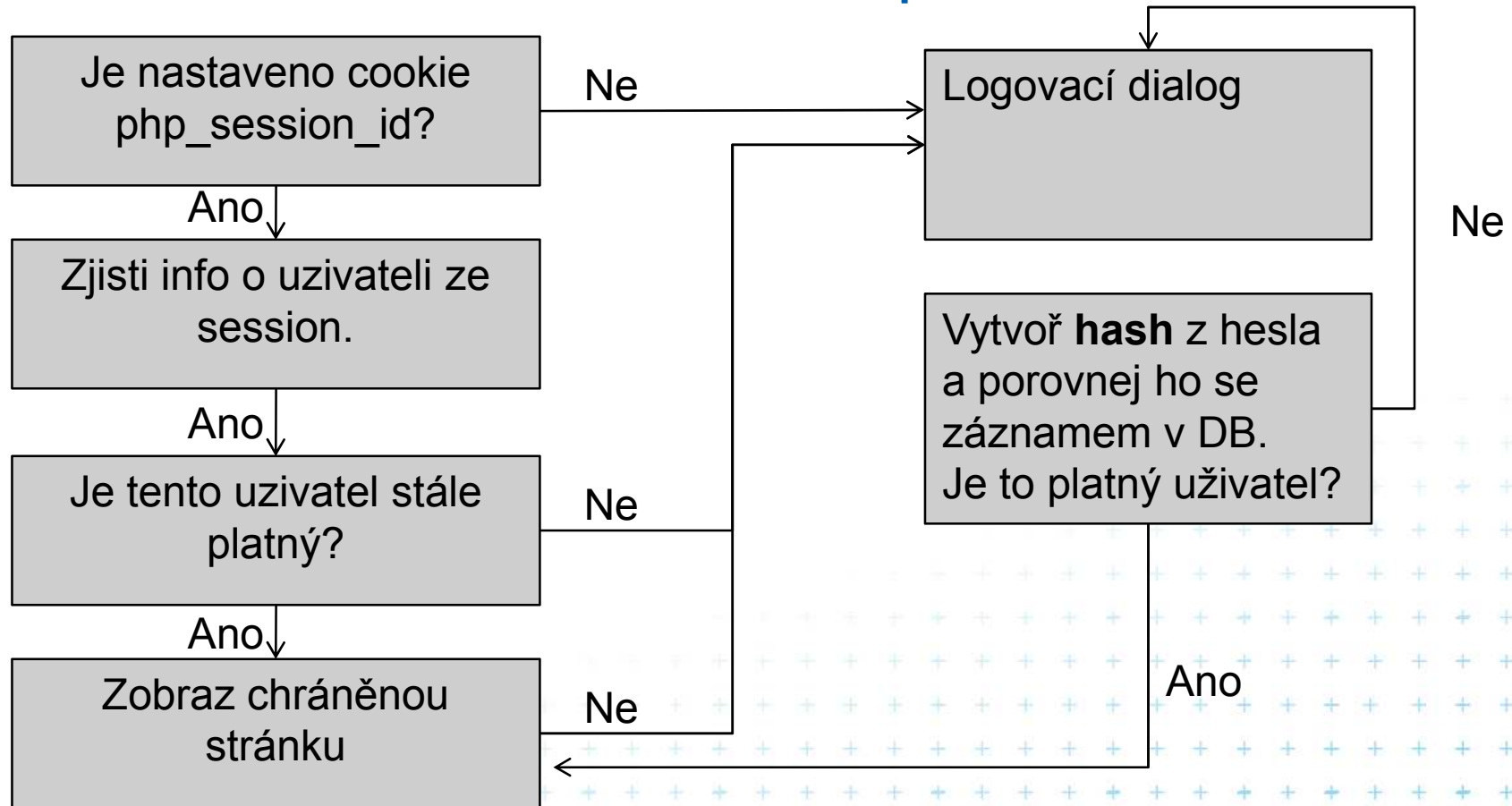
    foreach ($matches as $m) {
        $data[$m[1]] = $m[3] ? $m[3] : $m[4];
        unset($needed_parts[$m[1]]);
    }

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



Autentizace pomocí cookies, resp. session

- Řešíme to na úrovni PHP skriptu



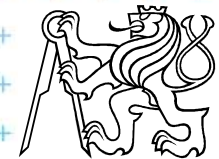
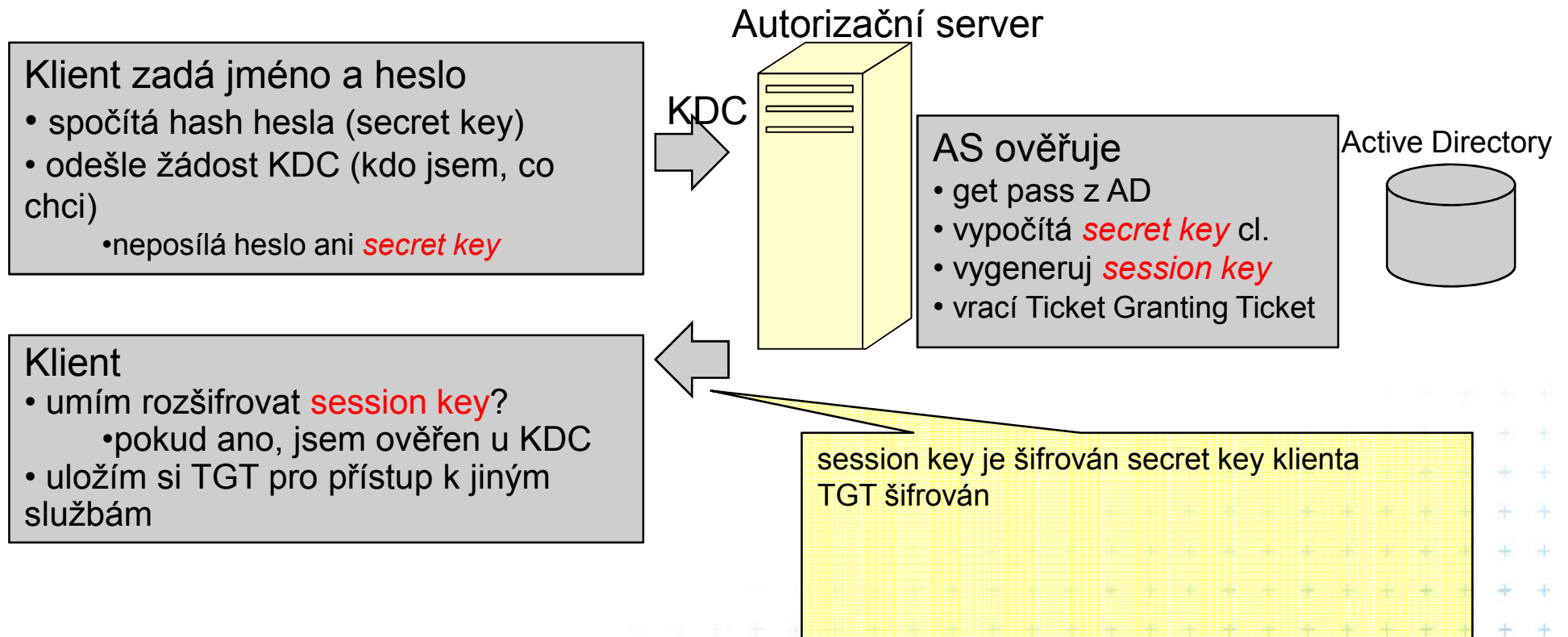
Ověření pomocí Kerberos protokolu

- Protokol umožňující SSO (single sign on)
- Bezpečný, rychlý
- Omezená skupina klientů

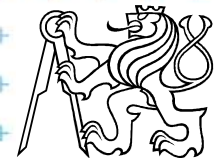
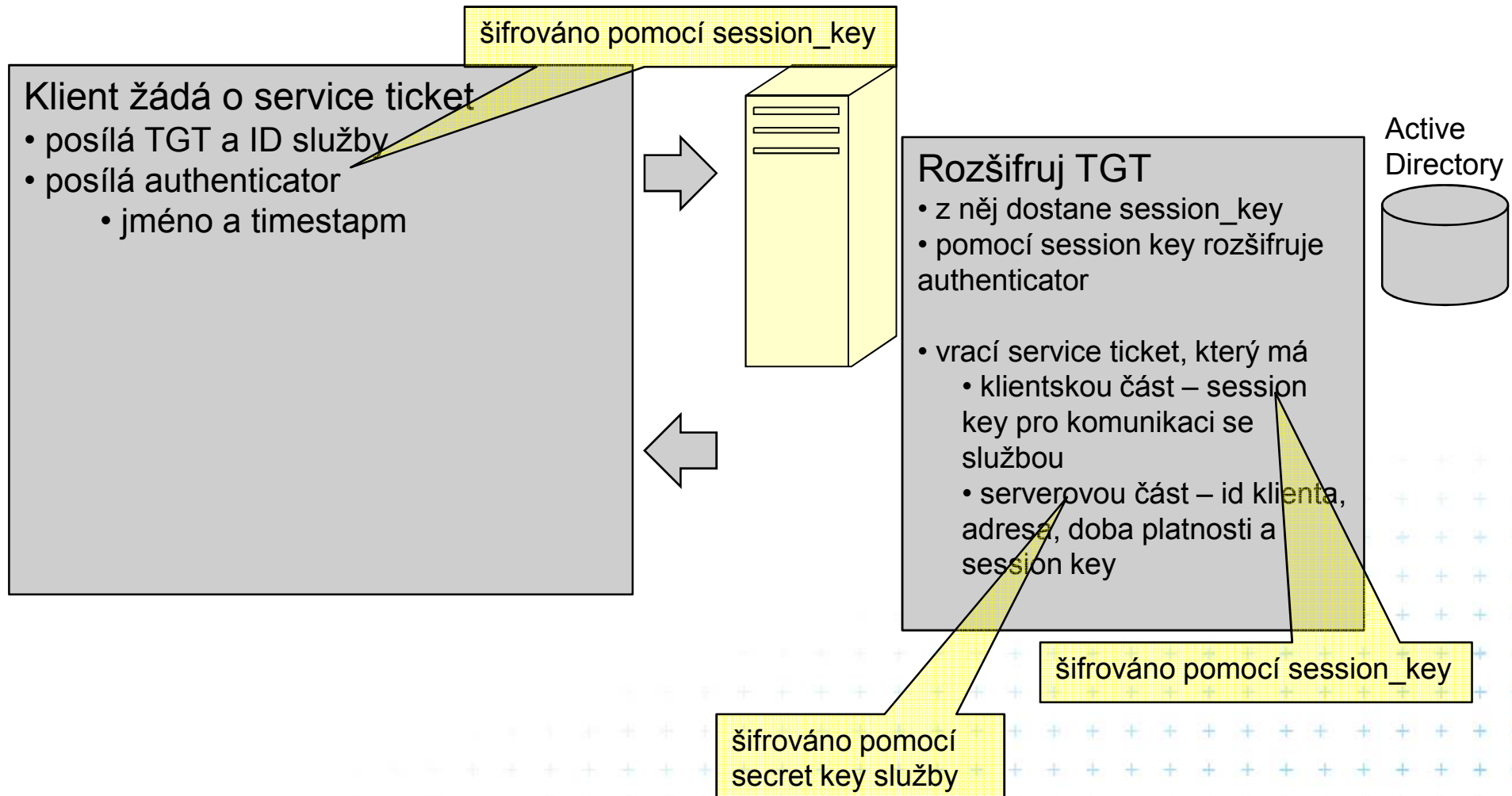


Kerberos – jak to funguje

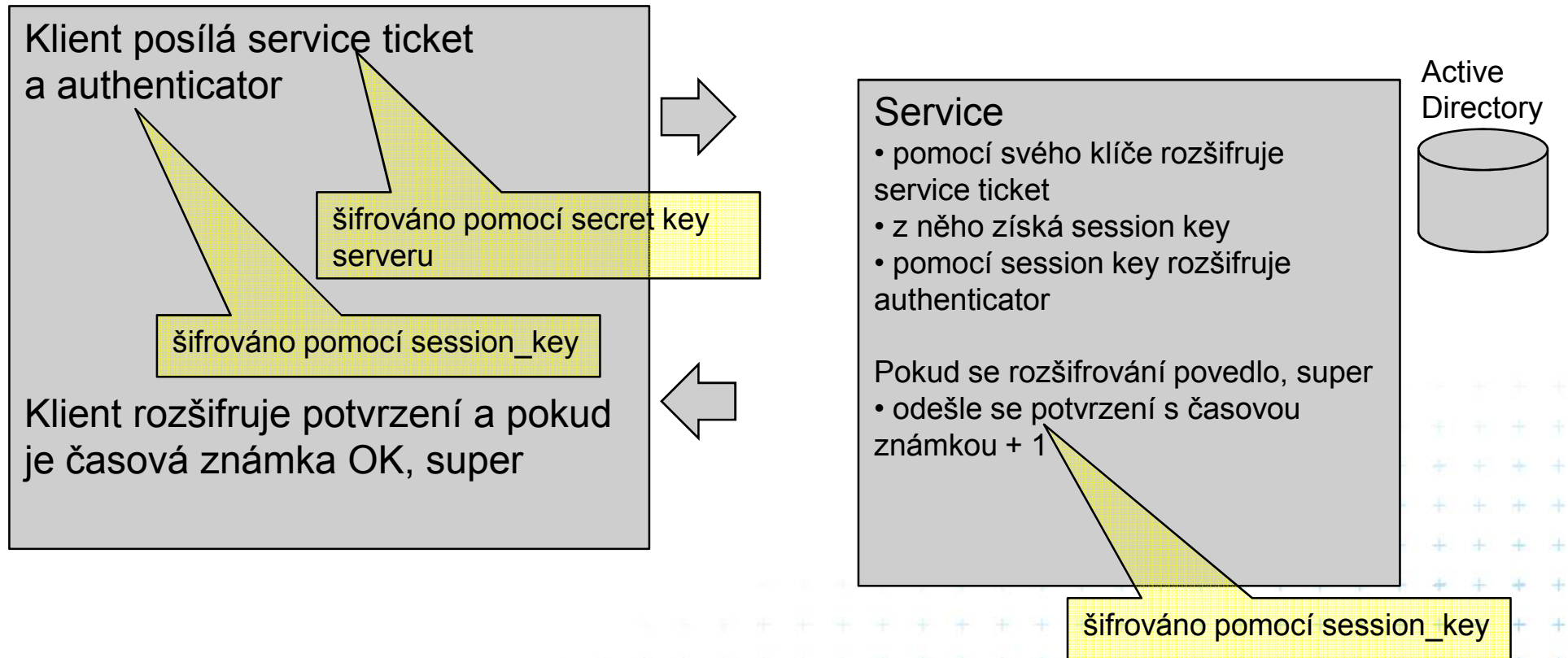
Počáteční autorizace u serveru

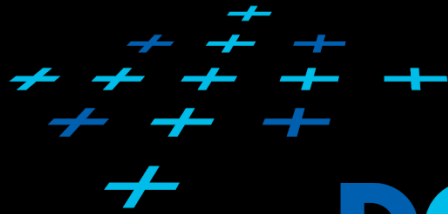


Kerberos – získání Service Ticket



Ověření u služby





DCGI

KATEDRA POČÍTAČOVÉ GRAFIKY A INTERAKCE

Pear = Hruška



Pear - hruška

- Systém pro implementaci a distribuci znovupoužitelných komponent (v PHP)
- Strukturovaná knihovna open-source (PHP) skriptů
- Systém pro distribuci skriptů a jejich správu
- Definiuje standard, jak psát PHP kód
- Další podpůrné prostředky
 - Web stránky
 - Mailing listy
 - Bug report
 - ...
 - ...



Co to umí

- Spousta dobře napsaných kódů
- Objektově orientované
- Dokumentované
- Umí se to samo nainstalovat

Kde to je

<http://pear.php.net>



PEAR Packages - Mozilla Firefox

http://pear.php.net/packages.php

Search for in the Packages

Main Support Documentation **Packages** Package Proposals Developers Bugs

List Packages Search Packages Statistics Channels

Packages (562) Filter by [PHP 4](#) [PHP 5+](#) All PHP Versions

<p>Authentication — 9</p> <p>Auth, Auth_HTTP, Auth_PrefManager, Auth_PrefManager2, ...</p>	<p>Benchmarking — 2</p> <p>Benchmark, test</p>	<p>Caching — 2</p> <p>Cache, Cache_Lite</p>
<p>Configuration — 1</p> <p>Config</p>	<p>Console — 7</p> <p>Console_Color, Console_CommandLine, Console_Getargs, Console_Getopt, ...</p>	<p>Database — 33</p> <p>DBA, DBA_Relational, DB_ado, DB_DataObject, ...</p>
<p>Date and Time — 25</p> <p>Calendar, Date, Date_Holidays, Date_Holidays_Austria, ...</p>	<p>Encryption — 14</p> <p>Crypt_Blowfish, Crypt_CBC, Crypt_CHAP, Crypt_DiffieHellman, ...</p>	<p>Event — 2</p> <p>Event_Dispatcher, Event_SignalEmitter</p>
<p>File Formats — 33</p> <p>Archive_Tar, Archive_Zip, Contact_AddressBook, File_Archive, ...</p>	<p>File System — 6</p> <p>File, File_Find, File_Mogile, File_SearchReplace, ...</p>	<p>Gtk Components — 4</p> <p>Gtk_FileDrop, Gtk_Styled, Gtk_VarDump</p>
<p>Gtk2 Components — 7</p> <p>Gtk2_EntryDialog, Gtk2_ExceptionDump, Gtk2_FileDrop, Gtk2_IndexedComboBox, ...</p>	<p>HTML — 41</p> <p>HTML_AJAX, HTML_BBCodeParser, HTML_Common2, HTML_Crypt, ...</p>	<p>HTTP — 15</p> <p>HTTP, HTTP_Client, HTTP_Download, HTTP_FloodControl, ...</p>

Najít: [Další](#) [Předchozí](#) [Zvýraznit](#) Rozlišovat velikost



Autorizace

- Chceme se „nestarat“ o pozadí autorizace
- ABSTRAKCE

