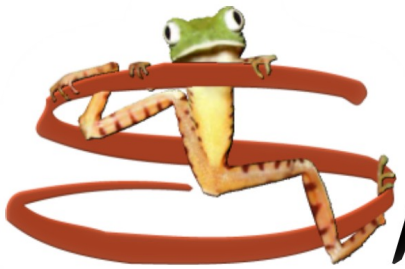


SkinaIT Solutions

Hoy to use Simple-SecREST library to develop a secure REST comunication.

Ing. Ricardo Naranjo Faccini, M.Sc.

2020-09-10

https://www.skinait.com/simple-secrest-Escritos-60/https://www.skinait.com/simple-secrest-Escritos-60/

Summary

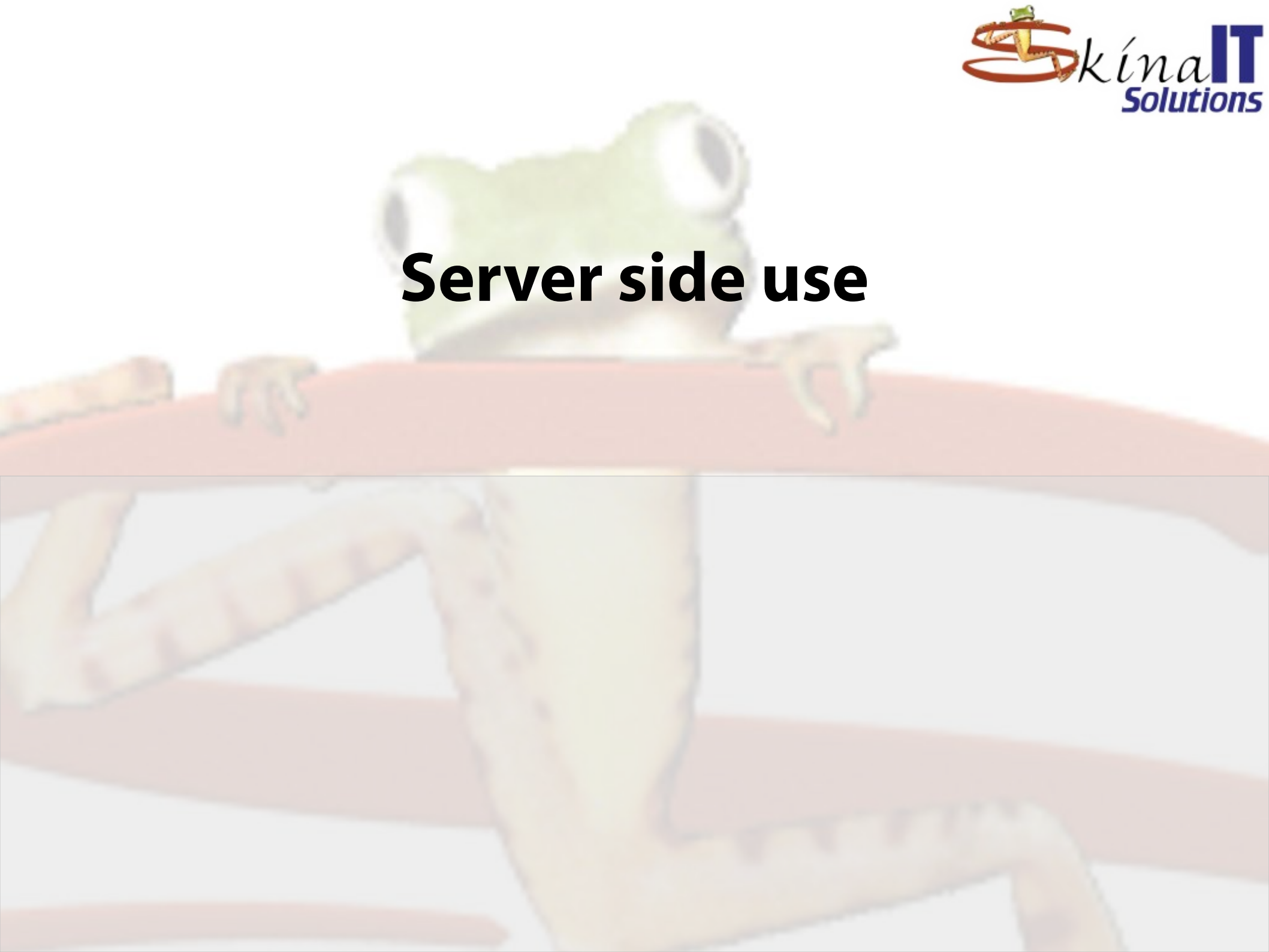
- Licence
- The library
- Server side use
- Client side use

Licence

- This is free software.
- Under LGPL Lesser General Public Licence.
- Developed by Ing. Ricardo Naranjo Faccini, M.Sc.
- Opened by Skina IT Solutions.
  - Columbian Software Factory

About the library

- GitHUB repository:
  - https://github.com/gramo44/Simple-SecREST
- Keeps safe data exchange in 4 times:
  - Handshake:
    - Sharing short duration RSA keys.
  - Keys expiration:
    - It generates a new pair of keys and the signature with which it is about to expire.
  - Sending access credentials {login, password}
    - Generates key hashmark combined with the current date and time.
  - Exchange of data after RSA validation and encryption with short-lived keys.



Server side use

Organize the proper directory tree

Link service.php with the services you want to provide.

```
$depurando = false; // true if you want debug messages.

$servidor = new mi_servicio("Path/to/external/directory"
                            , null
                            , 300  // customize in seconds the
                                   // key duration.
                            , $depurando);

$lista_blanca['metodo'] = array( "service_1" // Name of the
                               , "service_2" // services you want
                               , "service_3" // to provide.
                               , "service_4"
                               , "service_5"
                               );
$servidor->establecer_lista_blanca($lista_blanca);

$respuesta = $servidor->atender($_REQUEST);
```

Customize class in lib/mi_servicio.php

```
class my_service extends SR_REST {
    function M_REST_service_1($request)
    {
        $retorno = array( 'xxxx' => 0
                        , 'yyyy' => 0
                        , 'id_error' => 0
                        , 'error' => ""
                        );

        return $retorno;
    }
    // ...
    function M_REST_service_n($request)
    {
        $retorno = array( 'xxxx' => 0
                        , 'yyyy' => 0
                        , 'id_error' => 0
                        , 'error' => ""
                        );

        return $retorno;
    }
    // OBLIGATORY ABSTRACT METHODS
}
```

Customize class in lib/mi_servicio.php

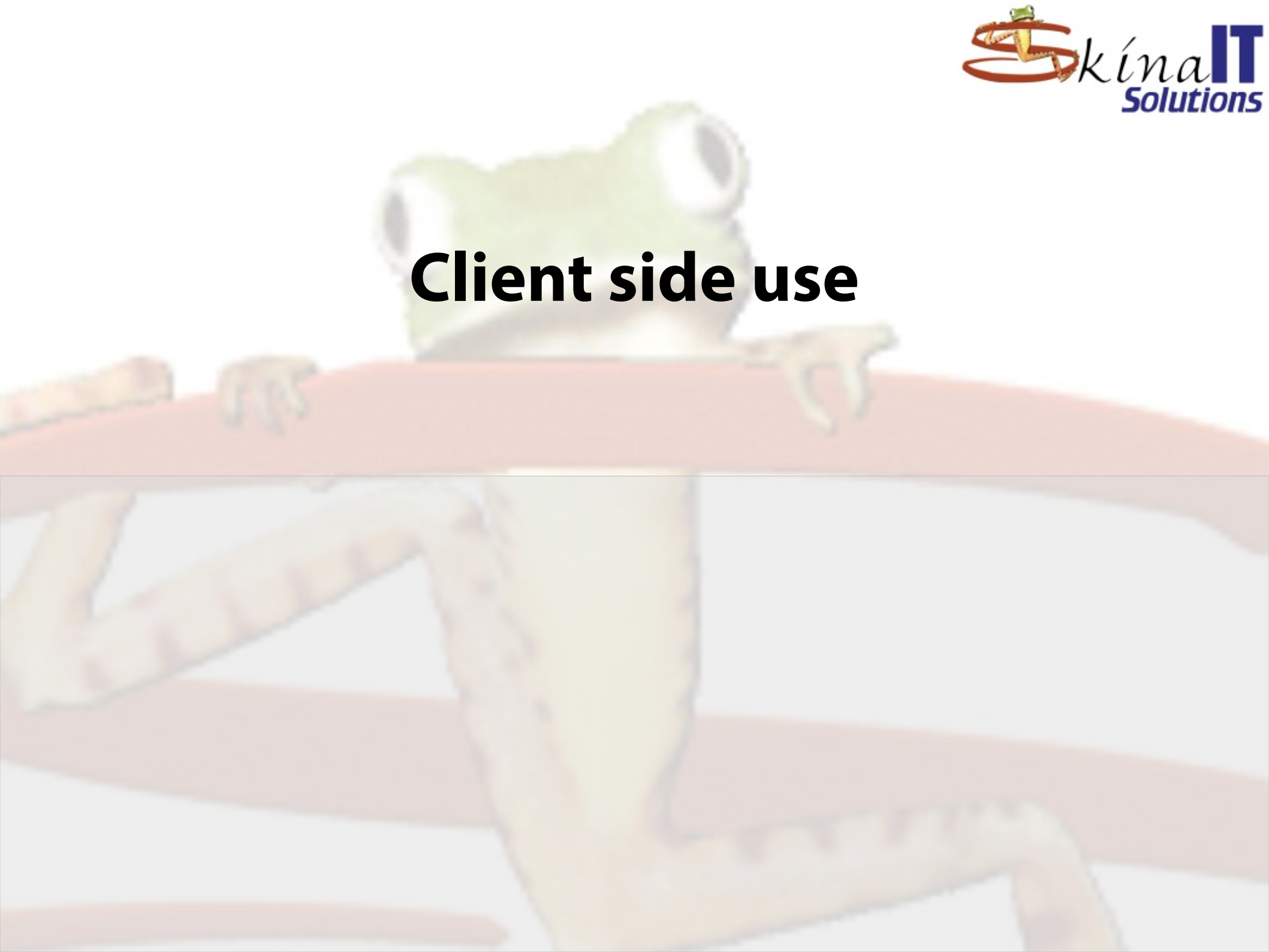
```
/*-----------------------------------------------------------------*/
function cargar_hash_de_clave($login) : string
/*******************************************************************
    @brief This function must return the sha512 checksum for the
    $login user's password, in order to be used to client authentication.

    INPUTS:
    @param $login user's login.
    OUTPUT:
    Password sha512 checksum
*******************************************************************/
```

Customize class in lib/mi_servicio.php

```
/*-------------------------------------------------------------------*/
function guardar_llave_publica_sesion($sesion, $pkey)
/*********************************************************************
@brief Stores persistently (into a database or file) a given session
code linked with a public key and its creation date.

Keys older than the customized duration ($this→duracion) must be erased
from this keyring.

INPUTS
@param $sesion alphanumeric code with length 13, the session ID.
@param $pkey The public key to be linked.
OUTPUT
bool: true -> on successfull storage.
*********************************************************************/
```

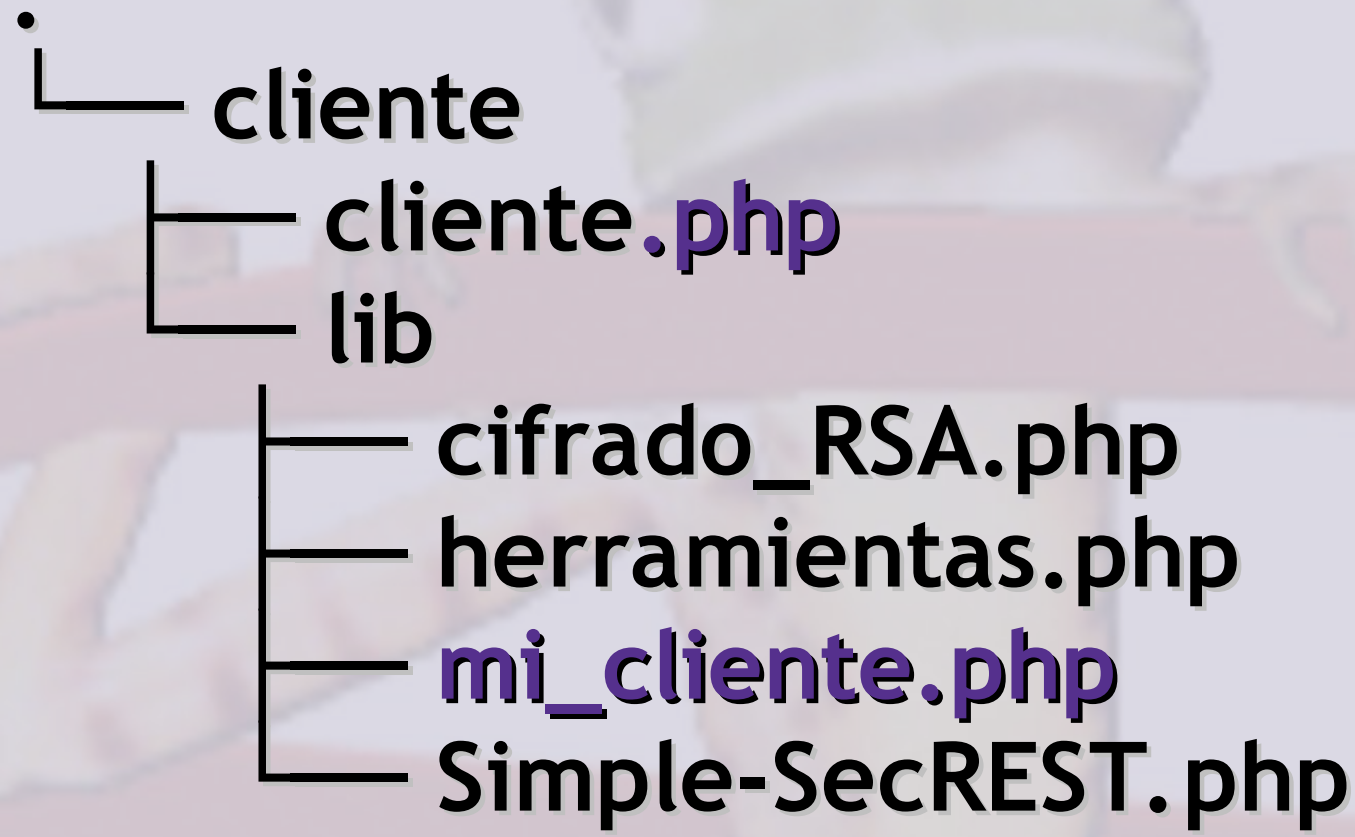
Customize class in lib/mi_servicio.php

```
/*-----------------------------------------------------------------*/
function cargar_llave_publica_sesion($sesion)
/*****************************************************************
@brief Verifies if the keyring stores a public key linked with the given
$session code stored more recently than $this->duracion.

This public key will be used to encrypt data to be sended to the client.

INPUTS
@param $sesion alphanumeric code, the session ID.
OUTPUT
string : The public key to be used with the session ID.
*****************************************************************/
```



Client side use

Organize the proper directory tree



(directorio externo con permisos de escritura para el cliente)

Customize class in lib/mi_cliente.php

```
class my_client extends CL_REST {
    function guardar_sesion_servicio($url, $sesion, $pkey) {
    /**************************************************************
    @brief Stores the session ID linked with the server, the public key and
    Its creation date.
    INPUTS
    @param $url The REST server location.
    @param $sesion The alphanumeric session ID.
    @param $pkey The public key for encrypt data to the REST server.
    **************************************************************/
        Instructions;
    }
    public function cargar_sesion_servicio($url) {
    /**************************************************************
    @brief Returns the last session ID linked to the REST server if it is
    Available.
    INPUTS
    @param $url The REST server location
    SALIDA
    Array with:
    The las session ID or null if not available.
    The public key for encrypt data to the REST server.
    **************************************************************/
        Instructions;
    }
}
```

Link cliente.php with the class wich uses the services provided.


```php
require_once("lib/mi_cliente.php");
require_once("lib/herramientas.php");

$url = "http://REST.server.url/path/to/RESTserver/servicio.php";
$login = "login";
$clave = hash('sha512', 'password');
$fecha = date("Y-m-d H:i:s");
$dir   = "/path/to/private/directory/with/write/permission";
$depur = false; // or true if you want debug messages.
$cliente = new mi_cliente($url, $login, $clave, $fecha, $dir, $depur);

$parametros['xxxx'] = "123456789";
$respuesta = $cliente->solicitar("service_1", $parametros);
print var_export($respuesta, true);
```

Thank you

Questions?

ventas@skinait.com

http://www.skinait.com