

# Using Google The Federated Way

Mihály Héder  
MTA SZTAKI ITAK

Eurocamp  
2009. november 18.

# Contents

- Intro of our Institute and Department
- Intro of our AAI system
- Google@osztaki
  - Apps for education
  - The Google Apps VO scheme
  - Backup

# I) SZTAKI, ITAK and what we do

# Introducing MTA SZTAKI

- Hungarian Academy of Sciences
- Computer and Automation Research Institute
- Around 300 employees, mainly research and development
- Like Fraunhofer, but smaller. Also, we didn't invent mp3.

# Introducing MTA SZTAKI ITAK

ITAK (Internet Technologies Applications Center) is a department of Institute SZTAKI, dealing with Internet technologies, developments, implementations, and research.

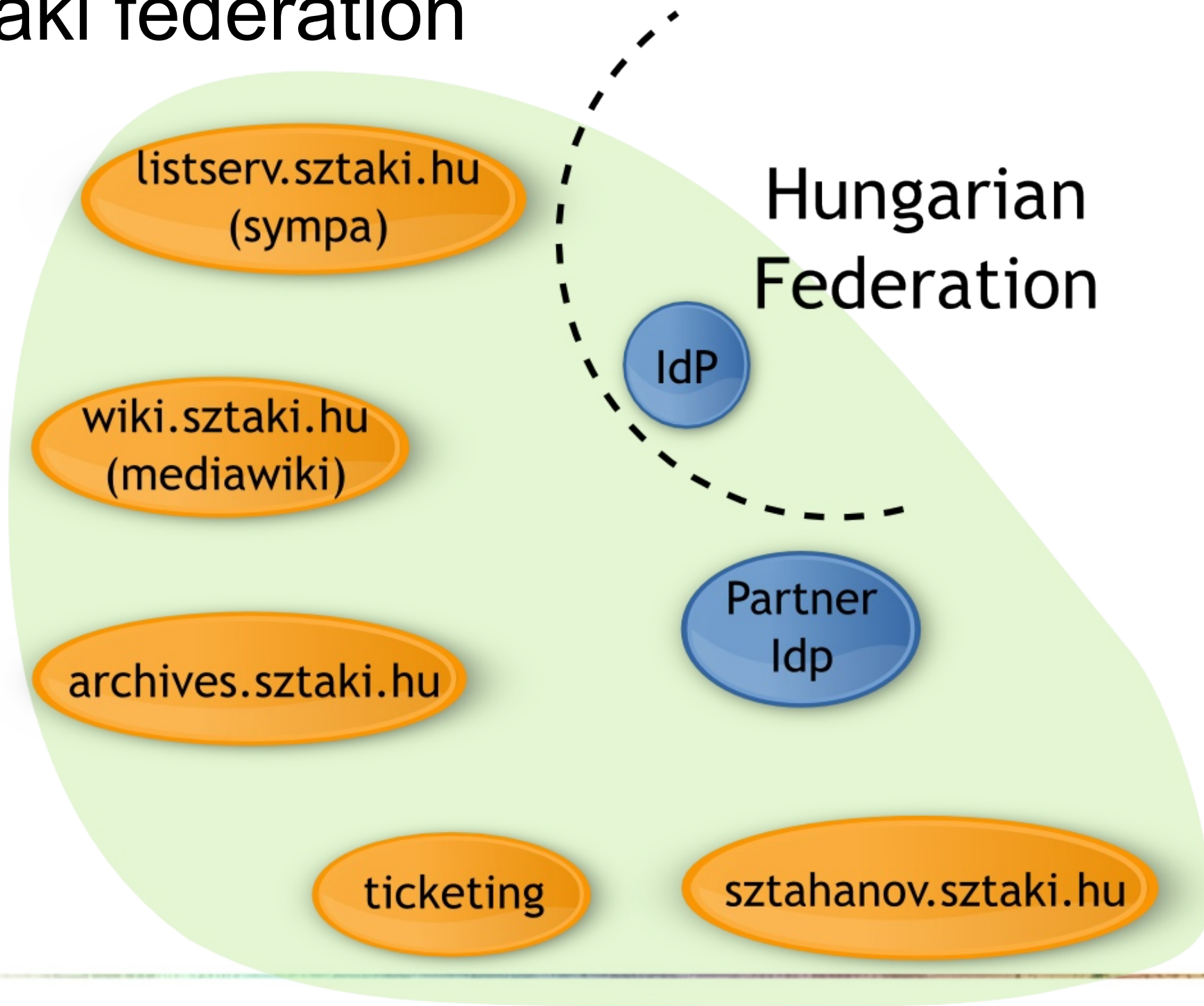
The main fields of activity:

- Datacommunications networks
- Scalable, highly reliable systems and Internet applications
- Authentication and authorization (federative) infrastructures
- Consultancy

# An impression of the Federation in SZTAKI

- Since 2006
- We have been using Shib 1.3x on both IdP and SP sides
- We've just migrated to simpleSAMLphp on the IdP side and plan to migrate most of the SP-s as well

# Sztaki federation



# The reasons for the platform change

- We have a tradition of implementing everything with LVS+GPFS cluster
  - We haven't been big fans of JGroups and HAProxy because the different architecture, complexity and extra management costs
  - We feel that Terracotta and java class instrumentation are just not our thing, basically for the same reasons
- We tried to exploit the capabilities of Spring framework and implement our own StorageService class but OpenSaml API has its own obstacles(StorageService<KeyType,ValueType> is too general to implement even with today's persistence APIs)
- We prefer sSphp's consent module to uApprove
- We want(ed) logout (now it is solved in Shib2, too)
- OpenID 1 support

# Fed Tech development

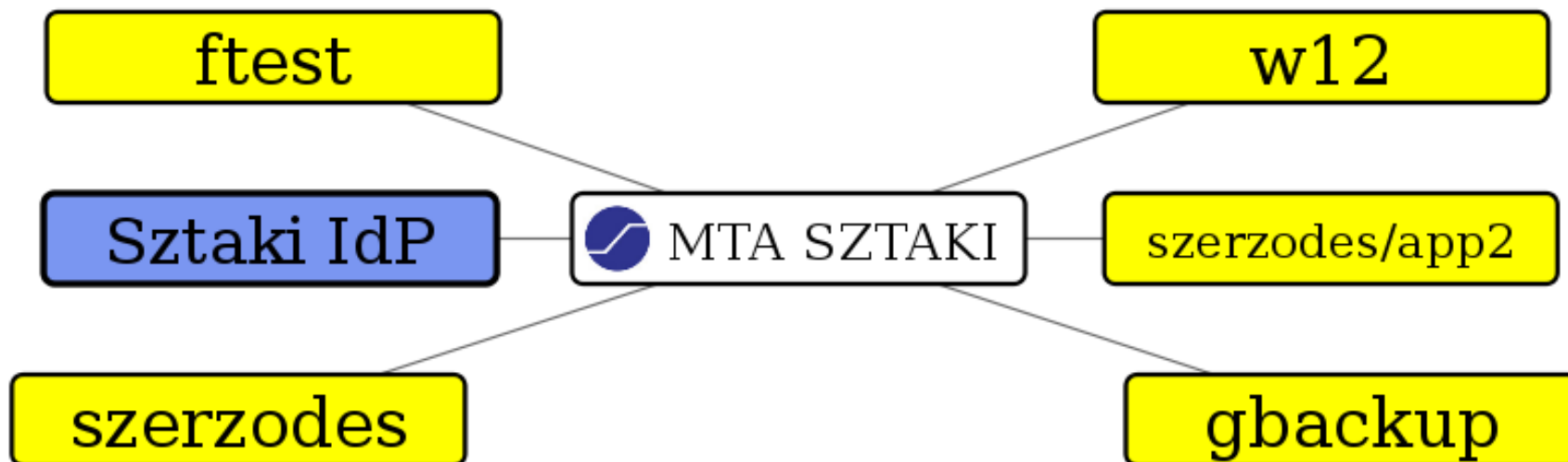
- IP Multimedia Subsystem - Diameter - Shibboleth: a solution for retrieving attributes from the mobile operator
- Carneades Contract Format: XML for representing contracts, eg.: user's consent
- XACML plans
- MetaView

# MetaView metadata visualizer

## Metadata + XSLT 2-> SVG+Javascript

- GOAL: visualize metadata as some kind of map
- Merging metadata files into one file:  
Embedding each file's outer *EntityDescriptors* element into a new *EntityDescriptors* element
- Now that we have only one file we can easily do the transformation
- We group the Entities by their *OrganizationName*. No organization name?-> Unknown Organization
- We use the *ContactPerson*, *ServiceName*, and *RequestedAttribute*, *ServiceDescription* elements when displaying an Entity
- We have additional extensions: public, EntityURL

# MetaView



## II) Google @ SZTAKI

# Google Apps for Education

## Benefits

- Everyone likes the gmail web interface
- 7 GB mail storage space for everyone  
(350\*7GB = 2,45 TB)
- Google docs, spreadsheets are very useful for collaboration
- Easy administration
- Cost reduction
- No ads in the Education edition





Search Mail

Search the web

[Show search options](#)  
[Create a filter](#)

[Compose Mail](#)

ESPN.com - [Sources: Philadelphia Eagles' Brian Westbrook likely out vs. Dallas Cowboys](#) - 2 hours ago

Web Clip < >

**Inbox (2140)**

[Starred](#) ★

[Sent Mail](#)

[Drafts](#)

[Follow up](#)

[Misc](#)

**Archive** Report spam Delete Move to ▾ Labels ▾ More actions ▾ [Refresh](#)

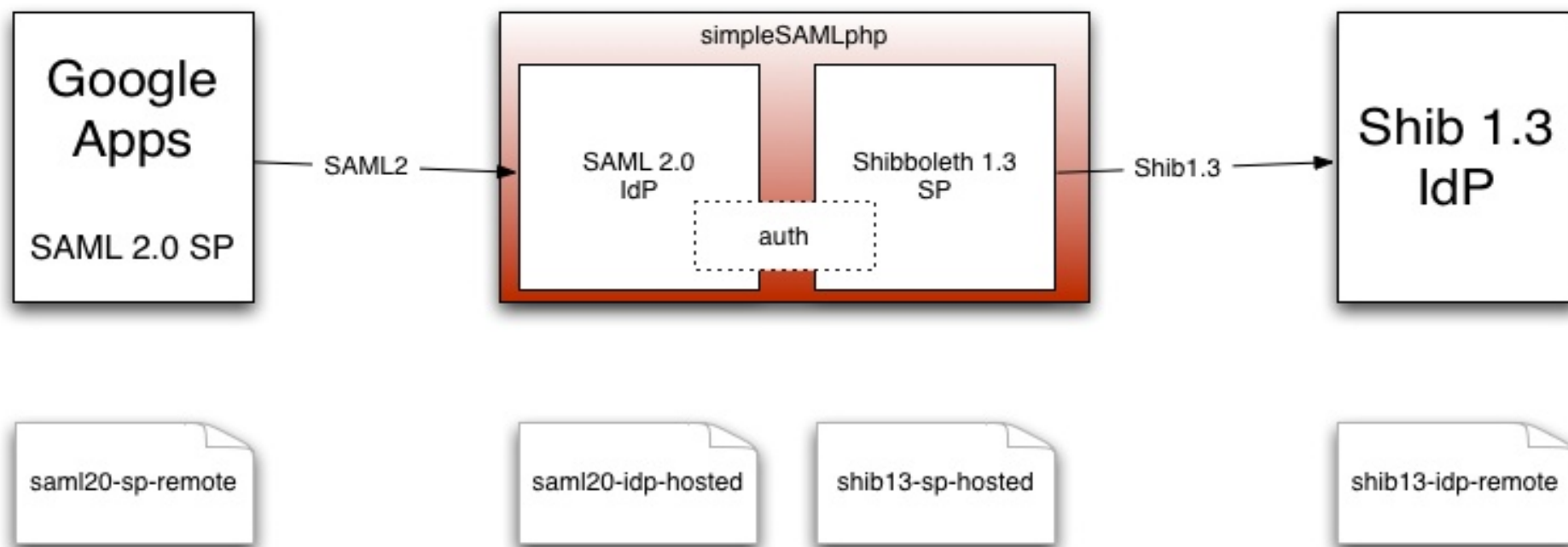
1 - 50 of 2147 [Older](#) > [Oldest](#) »

Select: All, None, Read, Unread, Starred, Unstarred

<input type="checkbox"/>	★ xsl-list-digest-help	xsl-list Digest 8 Nov 2009 06:10:00 -0000 Issue 2007 - xsl-list Digest 8 Nc	07:10
<input type="checkbox"/>	★ xsl-list-digest-help	xsl-list Digest 7 Nov 2009 06:10:00 -0000 Issue 2006 - xsl-list Digest 7 Nc	7 Nov
<input type="checkbox"/>	★ Szonja, Péter (3)	Re: [Phd2008] Fwd: Google Calendar teendők - sonia.odrovics@gmail.	7 Nov

Logo, domain management

# Shib1.3 IdP <- BRIDGE -> SAML2 SP



- We had to create the proper Metadata files
- The SAML 2.0 IdP uses the 1.3 IdP as Auth source
- SAML2 idp registration in google (Domain admin page)
- (Image taken from Andreas Solberg)

# User management

## SZTAKI

- There is a user subscription site which is an SP in our federation
- The site informs the user about the released attributes and requests consent
- After the consent is given we create the google user account through Zend GData API
- This is done by the privileged administrator user

## Google

- There is a self-administration site on the google side: you can change your password (which you don't on the web because of the federated access. But you use it for IMAP)
- Google asks for the users's consent on first login
- Admin site: User and Group Management
- email alias (xxx@g.sztaki.hu)

# User Management at SZTAKI

## 1. Subscription

Goal: Creating the User Account in Google

Zend GData API

Privileged User (administrator)

php code for creating a user

```
$service->createUser($username, $familyName,  
$givenName, $password);
```

```
$user->login->changePasswordAtNextLogin = true;
```

We ask for the user's consent for releasing the following attributes:

surname

given name

userid

# User Management at Google



Üdvözljük a(z) Computer and Automation Institute domainen!

Állítsa be a fiókját a(z) Computer and Automation Institute domainhez

A(z) Ön Computer and Automation Institute fiókjával hozzá férhet a domainjén engedélyezett hostolt szolgáltatásokhoz.

Név: Teszt Elek Vezetéknév

Bejelentkezési név: tesztelek@sztaki.hu

Válasszon jelszót:  Legalább 6 leütés Jelszó erőssége: **Erős**

Jelszó újra:

Nyelv: magyar

Írja be az alábbi képen látható karaktereket

Nem számít, hogy kis- vagy nagybetűk

Felhasználási feltételek: Olvassa el a lenti Felhasználási feltételeket

[Nyomtatható verzió](#)

Google Felhasználási feltételek

A Google üdvözlí Önt! A Google termékeinek, szoftvereinek, szolgáltatásainak, illetve webhelyeinek (a továbbiakban "Google szolgáltatásainak") használatával elfogadja az alábbi feltételeket és előírásokat, továbbá az időközönként esetleg megkapott minden egyéb szabályzatot, irányelvet és módosítást,

Azzal, hogy az „Elfogadom” elemre kattint, kinyilvánítja a fenti [Felhasználási feltételek](#), valamint a [Programszabályzat](#) és az [Adatvédelmi irányelvek](#) elfogadását.

Ne feledje, hogy a Google Alkalmazások a domain rendszergazdájának a tudomásával érhetőek el, és előfordulhat, hogy a domain rendszergazdája hozzá férhet a fiókadataihoz, köztük az e-mailjeihez is. Azt, hogy ezeket az adatokat a domain rendszergazdája milyen módon használhatja fel, a rendszergazda adatvédelmi irányelvei szabják meg.

Then google asks for accepting their Terms of Use

# User Management at SZTAKI

## Google password reset

Goal: to enforce the change of password stored at google

```
$user->login->changePasswordAtNextLogin = true;
```

After issuing this the user will be asked for changing the password

=> <http://framework.zend.com/manual/en/zend.gdata.gapps.html>

# User Management at SZTAKI

Deleting a user (eg. employee has left the organization)

```
$service->deleteUser($username);
```

=> <http://framework.zend.com/manual/en/zend.gdata.gapps.html>

# Result

- Calendar
- Resource (room) allocation (gcal)
- Ultra-light static home pages
  - coginfo.sztaki.hu,
  - eduroam.sztaki.hu,
  - szeminarium.sztaki.hu,
  - terem.sztaki.hu
- Office apps
- Glinks, tinyurl a la google
- Gtalk
- Gmail and Glabs
- Start page

=> <https://services.google.com/apps/site/overview/index.html>

# Result

But we don't have:

- [video.google.com](http://video.google.com) (not in Hungary)
- [picasaweb.google.com](http://picasaweb.google.com)
- [reader.google.com](http://reader.google.com)
- [maps.google.com](http://maps.google.com)
- ...

# Our Plans

- SAML 2.0 IdP
  - No bridge needed, easier maintenance
  - Failover (memcache, or GPFS)
  - Consent management
- Google Talk <-> Sztaki Asterisk

# Keeping the Bridge...

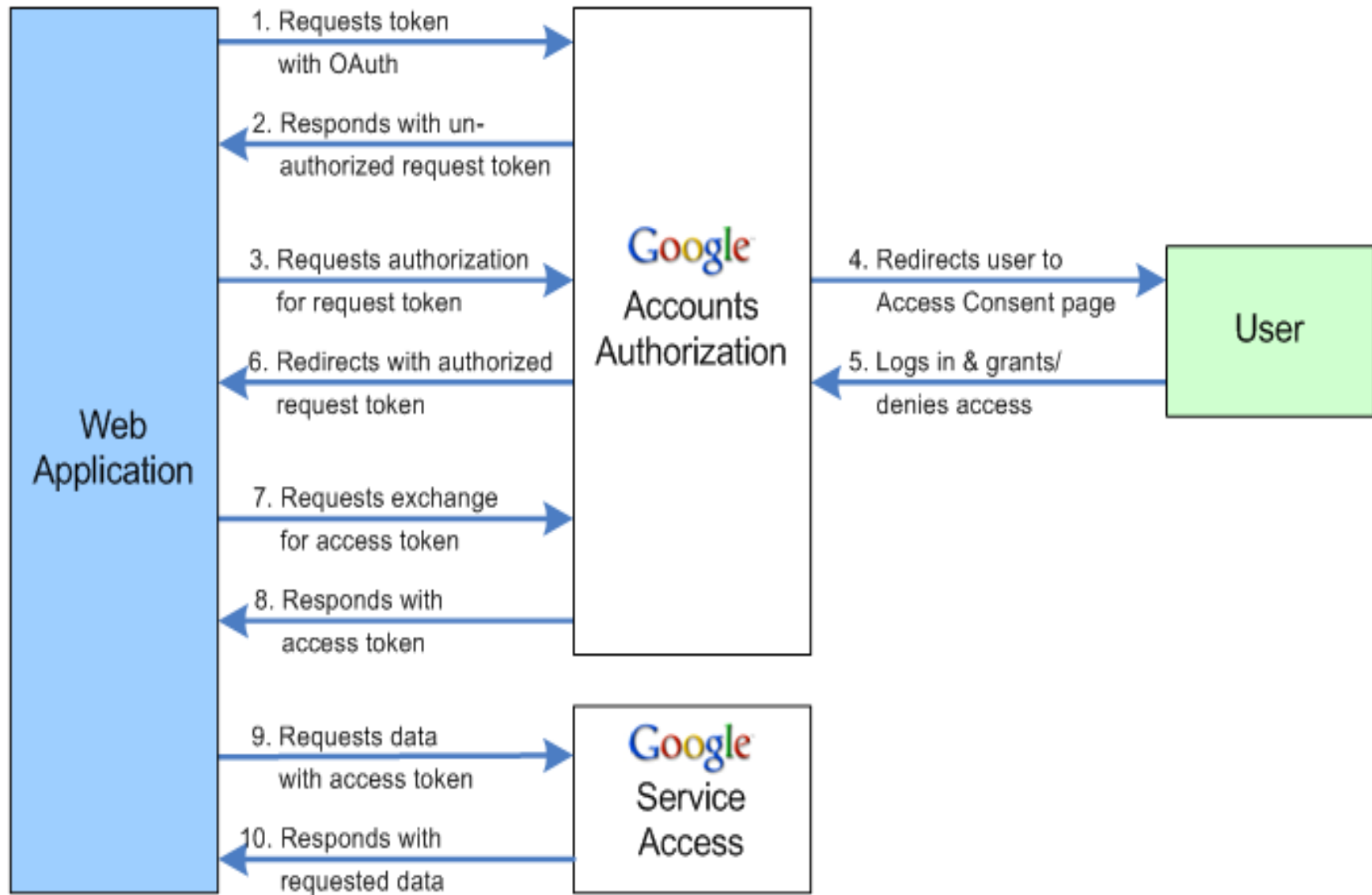
- It might makes sense to keep the bridge:  
This way we can implement a Virtual Organization based on Google Apps
- Homeless Users can use the google Account, others authenticate trough the bridge
- Only domain name needs to be registered
- Drawback: there is no SSO in the Google Apps Standard Edition: we have to pay 40€/year/person

## II/2) Domain Backup for Google

# Domain Backup for Google

- Sometimes when Google was not accessible we felt uncomfortable
- We decided that we need backup from our stuff stored in Google
- There are backup solutions for individual users but we wanted automated full domain backup.
- There are API-s in various languages for retrieving data from google - we choose the Zend gdata API (php)
- There is a brand new authentication method for APIs, called OAuth.
- There are two kinds of OAuth: Three legged (requires user interaction) and two legged

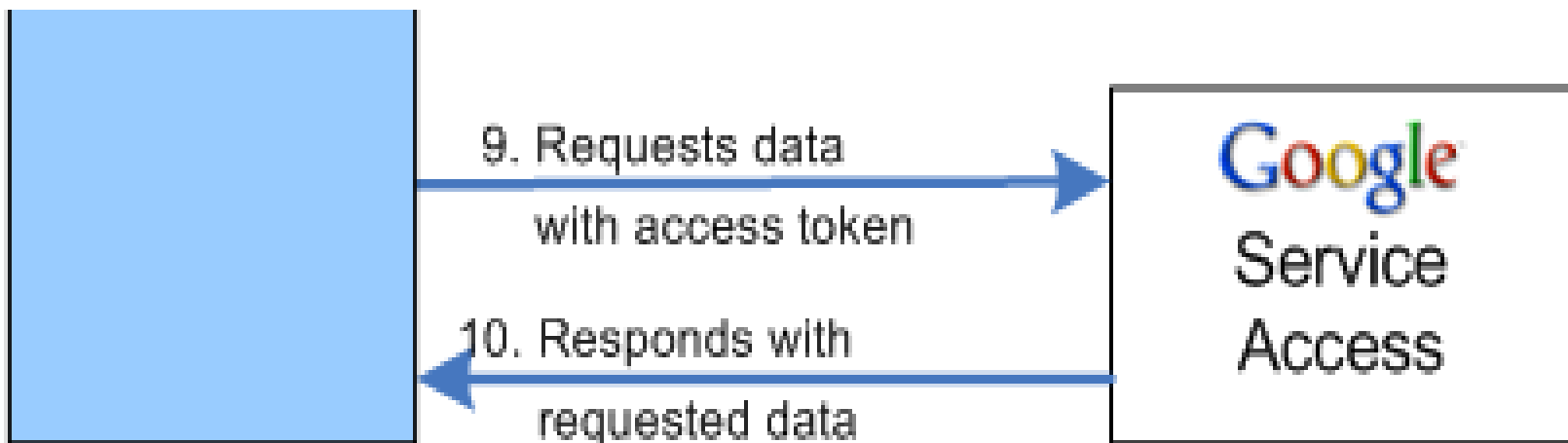
# Three-legged OAuth



- We can't use this because user interaction is needed

# Two-legged OAuth

- Also called Signed Fetch or Phone Home
- You could use either RSA-SHA1 or HMAC-SHA1
- No user interaction needed
- User id is provided in `xoauth_requestor_id`
- The number of tokens released by google is limited
- We must register a certificate in the Google Admin page, or you will get a key and consumer certificate



# RESTFul Atom API

- For retrieving data we use the google data API which is based on atom publishing standard and accessed in a RESTFul Way: GET, POST, PUT, etc.
- The Namespaces are mixed
- We can list, retrieve, and upload content, manage users, etc.

# What our backup app does

- There is an API we created for backup functions
- There is a web frontend based on this API
- There is a self-managed part of the web frontend, where users can start backups, or download the stored files
- There is an admin part of the web frontend. Here we can start full domain backups, and run them in the background
- Upon full domain backup the API always retrieves the list of the current users
- Using this list we download everything
- We can use the backup API from other programs
- One particular program is a simple php script which retrieves the full domain and is started with cron regularly

# Screenshot



## Adminisztrátori funkciók:

Mutasd a felhasználókat

Mutasd az összes naptárat

Bejelentkezve mint [merlin@sztaki.hu](mailto:merlin@sztaki.hu)

Admin jogosultággal

Mutasd a fájljaimat

Mutasd a naptárjaimat

A parancsok háttérben való futtatása

Docs biztonsági mentése

Contacts biztonsági mentése

Naptáraink biztonsági mentése

Backup MOST!

Mutasd a háttérfolyamataimat

[Újjelentkezés](#)

## Sztaki Google Backup tools

### Felhasználók listája

Nincs lekérdezés - használja a baloldali menüsáv gombjait

### Fájlok listája

#### merlin@sztaki.hu backup fájljainak listája

[Jelöld ki mindet!](#) [Töröld ki mindet!](#)

Parancs(ok) háttérben való futtatása

Kijelölt fájlok törlése

Mehet

Megjelenített sorok: 1-10 /

< |< Page 1 of 3 >| >

< Mutasd mindet >

Fájl neve	Backup időpontja	Ki indította a backupot	A backup időigénye (secundum)
<a href="#">sztaki.hu_88oi9m3siq4juutfkto9fiiei0%40group.calendar.google.com.zip</a>	2009-10-19 11:41:55	merlin@sztaki.hu	8.17
<a href="#">Contacts_2009-10-19-11-41-34.zip</a>	2009-10-19 11:41:34	merlin@sztaki.hu	0.01
<a href="#">sztaki.hu_88oi9m3siq4juutfkto9fiiei0%40group.calendar.google.com.zip</a>	2009-10-19 11:08:27	merlin@sztaki.hu	8.38
<a href="#">sztaki.hu_88oi9m3siq4juutfkto9fiiei0%40group.calendar.google.com.zip</a>	2009-08-31	namarsok@sztaki.hu	5

# Concluding Thoughts

- +With Google you get high quality web-based apps for low costs
- In return you have to trust them that they keep your data accessible and do not use it in ways you won't allow
- +With domain backup you access your data when google is down or lost them (but you still need to trust)
- If you don't have your own infrastructure you need to trust someone anyway

Thank you for your  
attention!



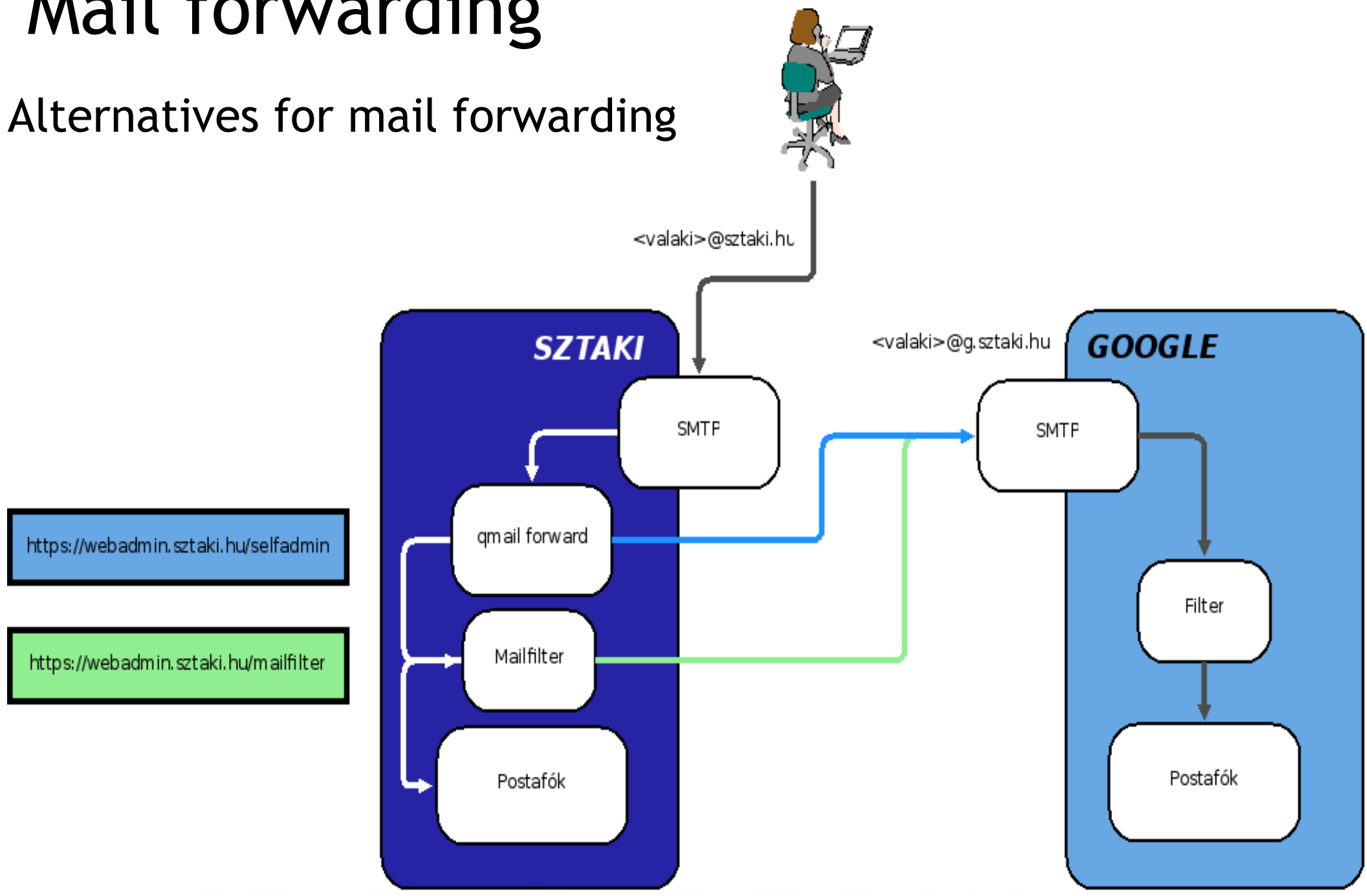
**MTA SZTAKI**  
COMPUTER AND AUTOMATION  
RESEARCH INSTITUTE  
HUNGARIAN ACADEMY OF SCIENCES

<http://itak.sztaki.hu/>  
[mihaly.heder@sztaki.hu](mailto:mihaly.heder@sztaki.hu)

# Additional slides

# Mail forwarding

## Alternatives for mail forwarding



# Google SSO configuration



Google Apps for sztaki.hu - Education Edition

Search accounts

Search Help Center

gyufi@sztaki.hu [Inbox](#) [Calendar](#) [Help](#) [Sign out](#)[Dashboard](#)[Users and groups](#)[Domain settings](#)[Advanced tools](#)[Support](#)[Service settings](#)[« Back to Advanced tools](#)

## Set up single sign-on (SSO)

To set up SSO, please provide the information below. [SSO Reference](#)

 **Enable Single Sign-on**

### Sign-in page URL \*

URL for signing in to your system and Google Apps

### Sign-out page URL \*

URL to redirect users to when they sign out

### Change password URL \*

URL to let users change their password in your system

### Verification certificate \*

A certificate file has been uploaded-[Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. [Learn more](#)

 **Use a domain specific issuer**

This must be checked if your domain uses an IDP Aggregator to handle SAML requests.

If enabled, the issuer value sent in the SAML request will be **google.com/a/sztaki.hu** instead of simply **google.com** [Learn more](#)

### Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network.

Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16)

For ranges, use a dash. Example: (64.233.167-204.99/32)

All network masks must end with a CIDR. [Learn more](#)

# Remote SAML2.0 SP entity

```
$metadata = array(  
    'google.com' => array(  
        'ForceAuthn' => true,  
        'AssertionConsumerService' => 'https://www.google.com/a/sztaki.hu/acs',  
        'spNameQualifier' => 'google.com',  
        'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:email',  
        'simplesaml.nameidattribute' => 'urn:mace:dir:attribute-  
def:eduPersonPrincipalName',  
        'simplesaml.attributes' => false  
    )  
);
```

# Local SAML2.0 IdP entity

```
$metadata = array(  
    // The SAML entity ID is the index of this config.  
    'idp.sztaki.hu' => array(  
  
        // The hostname of the server (VHOST) that this SAML entity will use.  
        'host'          => 'googlebridge.sztaki.hu',  
  
        // X.509 key and certificate. Relative to the cert directory.  
        'privatekey'    => 'googlebridge.sztaki.hu.key',  
        'certificate'   => 'googlebridge.sztaki.hu.crt',  
  
        // Authentication plugin to use. login.php is the default one that uses LDAP.  
        'auth'          => 'shib13/sp/initSSO.php',  
        'authority'     => 'shib13'  
    )  
);
```

# Local Shib1.3 SP entity

```
$metadata = array(  
    'googlebridge.sztaki.hu' => array(  
        'host' => 'googlebridge.sztaki.hu'  
    )  
);
```

# Remote Shib1.3 IdP entity

```
$metadata = array(
```

```
  'https://idp.sztaki.hu/shibboleth-sztaki' => array(
```

```
    'SingleSignOnService' => 'https://idp.sztaki.hu/idp-sztaki/SSO',
```

```
    'certFingerprint' => '2028f5b3543109674793771b32d6a61b7f973510'
```

```
  ),
```

```
);
```