
SWITCH

The Swiss Education & Research Network

AAI - PAPI
24. September 2002



Rolf Gartmann
SWITCH Security Group

- **Introduction PAPI**
- **Requirements leading to development of PAPI**
- **Architecture of PAPI**
- **SWITCH Test Installation**
- **Requirements for PAPI Installation**
- **Live Demo**
- **Behind the Scene**
- **Documentation**
- **Questions & Discussion**



- **PAPI: Point of Access to Providers of Information**
- **Built at rediris.es (Spanish National Research Network)**
- **Mainly developed (and still developing) by:
Rodrigo Castro-Rojo & Diego R. Lopez**
- **Current version 1.1.0
next version should be available end of September**

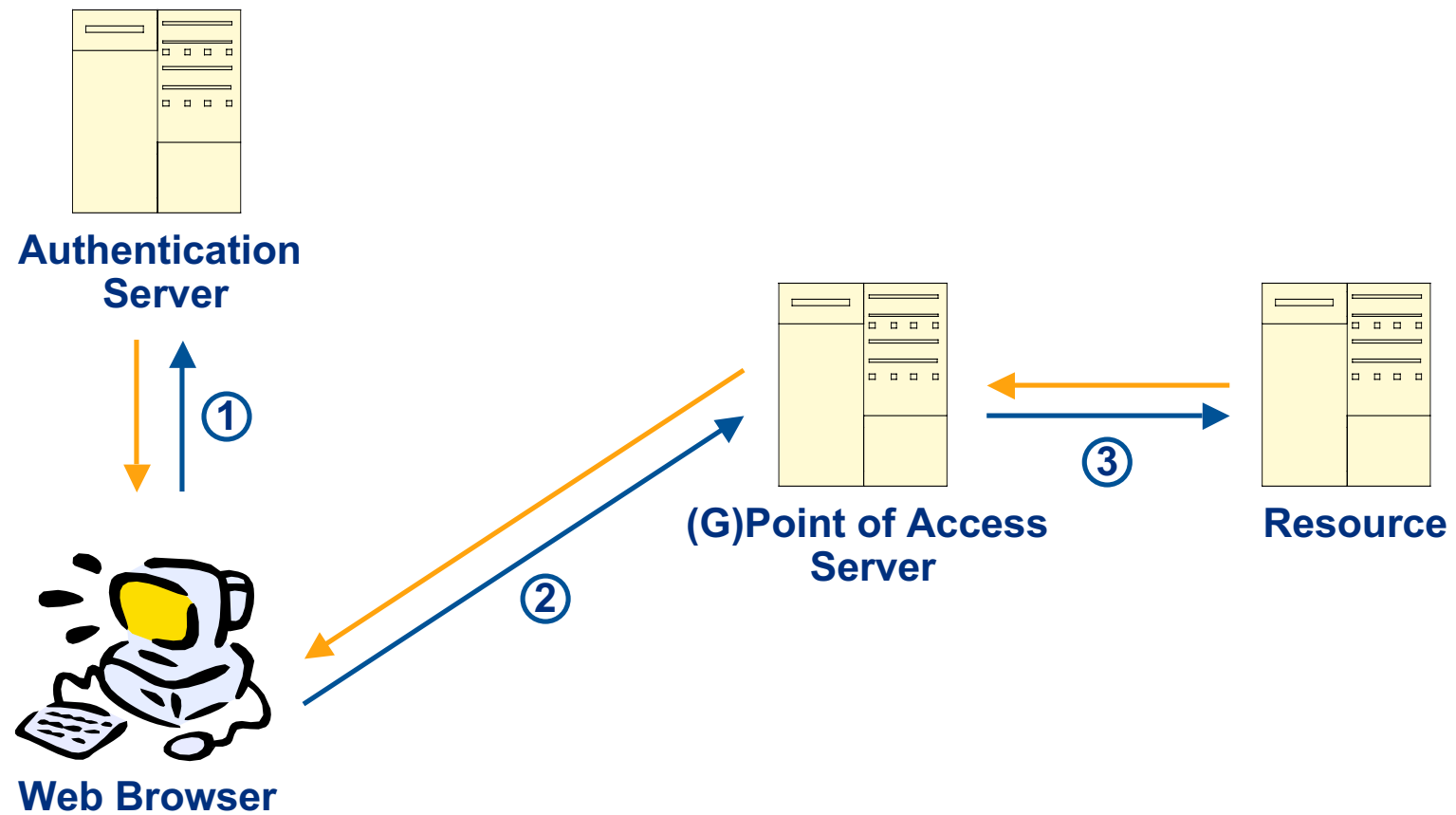


- **Access control independent from IP origin**
- **Upon successful local authentication, access must be granted during a configurable period of time to the services that the user is authorized**
- **User mobility**
- **Transparency to the user**
- **Compatibility with other commonly employed access control systems**
- **Compatibility with Netscape/MSIE/Lynx browsers**
- **Privacy at the user level, while easing the collection of statistics by providers**

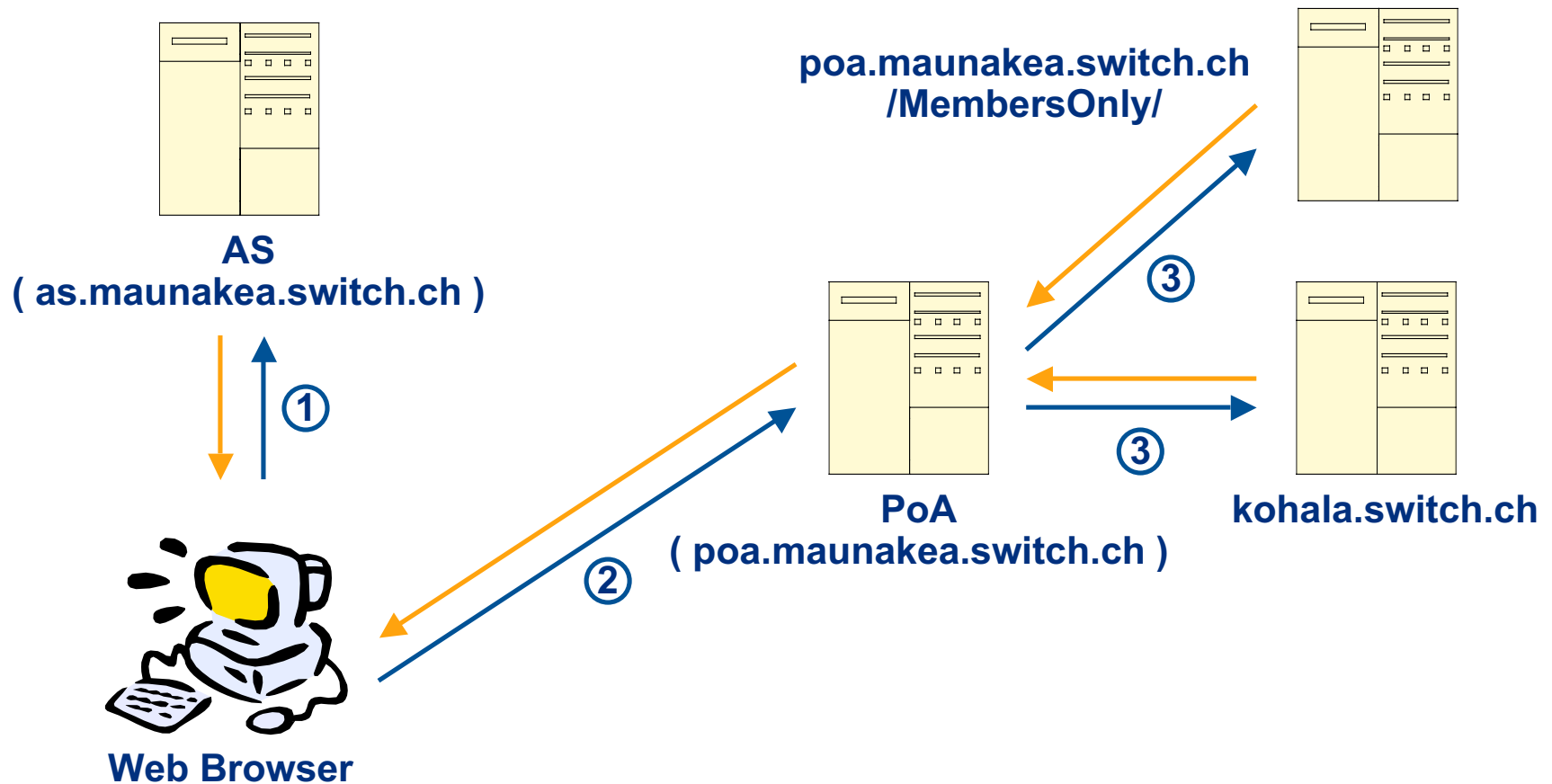
(slide based on PAPI presentation at Terena Networking Conference 2001)



PAPI - Architecture



PAPI - SWITCH Test Installation



General

- heavily based on Apache (including mod_perl), Perl and openssl
- Perl (≥ 5.004) & additional Perl Modules (DB_File, MIME::Base64, URI::Escape, Convert::ASN1)



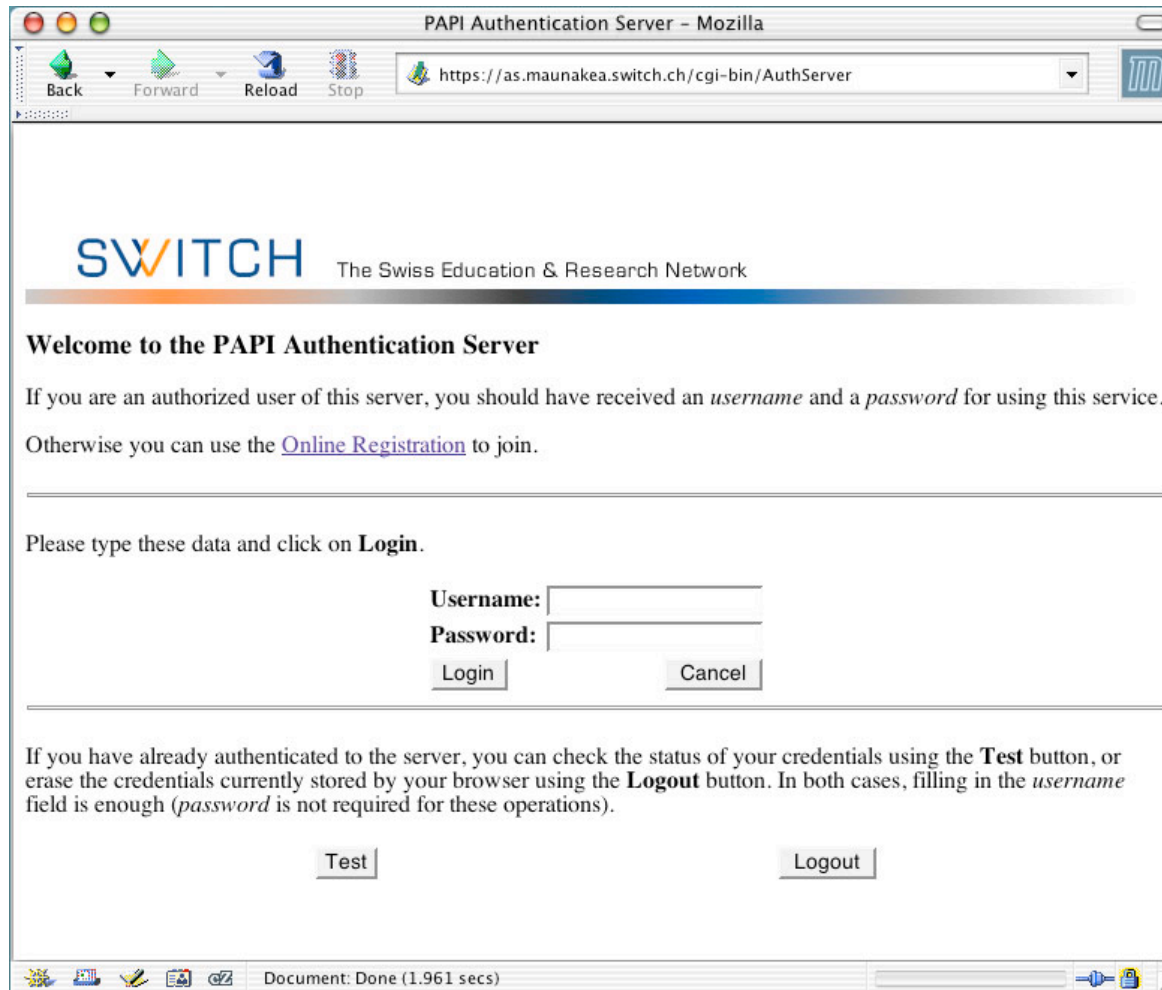
AS

- Apache ($\geq 1.3.8$)
- Additional Perl Modules
(CGI_Lite and optional
Sys::Syslog, Net::LDAP, Net::POP3)

PoA

- Apache & mod_perl (≥ 1.20)
- Additional Perl Modules
(Data::Dumper, HTML::TokeParser, HTTP::Cookies,
LWP::UserAgent, MLDBM, MLDBM::Sync)





The screenshot shows a Mozilla browser window titled "PAPI Authentication Server - Mozilla". The address bar contains the URL "https://as.maunakea.switch.ch/cgi-bin/AuthServer". The page content includes the SWITCH logo and tagline, a welcome message, a login form with "Username:" and "Password:" fields, and "Login" and "Cancel" buttons. Below the login form, there is a "Test" button and a "Logout" button. The status bar at the bottom indicates "Document: Done (1.961 secs)".

SWITCH The Swiss Education & Research Network

Welcome to the PAPI Authentication Server

If you are an authorized user of this server, you should have received an *username* and a *password* for using this service. Otherwise you can use the [Online Registration](#) to join.

Please type these data and click on **Login**.

Username:

Password:

If you have already authenticated to the server, you can check the status of your credentials using the **Test** button, or erase the credentials currently stored by your browser using the **Logout** button. In both cases, filling in the *username* field is enough (*password* is not required for these operations).

Document: Done (1.961 secs)



- **Browser (cookies)**
- **DNS(remote re sources & naming conventions)**
- **Configuration (AS, PoA, GPoA)**
- **Pitfalls, Tips & Tricks**



Users

user::ID::PASSWORD::ALT::GROUPLIST::SITELIST

Groups

group::ID::ALT::SITELIST

Site

site::ID::DESC::POA::POAURI::TTL::SERVICE::LOCATION

See also

maunakea.switch.ch/PAPI/#authentication%20server



AS - User Configuration - Example

```
# Users (group groupAAI)
user::rolf::aaLqSPyNHg.vM::::groupAAI::
user::christoph::actgYpyNHg.vM::::groupAAI::
# Groups
group::groupAAI::groupAAI::sitePAPIzed,siteKohala
site::sitePAPIzed::SWITCH
  PAPIzed::http://poa.maunakea.switch.ch::::1800::VHO-T-
  AS::/papized/
site::siteKohala::Kohala
  (remote)::http://papized.kohala.switch.ch::::1800::remote:
  :/papized/
```



```
<Location /papized>  
  PerlSendHeader On  
  PerlAccessHandler PAPI::Main  
  <PAPI_Local>  
    Server VHO-T-AS  
    Debug 1  
    # PAPI_Filter student  
  </PAPI_Local>  
</Location>
```



- See FAQ at (specially about installation issues):
<http://www.rediris.es/app/papi/dist/gb/PAPI-faq.html>
- CGI_Lite is a prerequisite for the PAPI AS part.
they changed the package in the current 2.0 version and
must now be included with:
use CGI::Lite
and therefore:
my \$cgi = new CGI_Lite ();
has to be .. new CGI::Lite ();
- In set_parameters in ApachePoA.pm
\$self->{'ApacheRequest'} = \$r;
should be set earlier, otherwise logging is not working
properly



- How to integrate ?
- What kind of interface is available ?
- Hcook_Handler

- The 'notes' table is for notes from one module to another, with no other set purpose in mind...
(from include/httpd.h)

```
$r->notes( $key, [$value] )
```

Return the value of a named entry in the Apache notes table, or optionally set the value of a named entry. This table is used by Apache modules to pass messages amongst themselves. Generally if you are writing handlers in mod_perl you can use Perl variables for this.

```
$r->notes("MY_HANDLER" => OK);  
$val = $r->notes("MY_HANDLER");
```

Will return a HASH reference blessed into the Apache::Table class when called in a scalar context with no "key" argument. This requires Apache::Table.




```
$papi_info = apache_note("PAPIHcook");
if ( strlen($papi_info) > 0 ) {
    error_log("Hcook: $papi_info",0);
    if ( ereg(":(.+)", $papi_info, $arr) ) {
        $REMOTE_USER = $arr[1];
        error_log("user extracted: $REMOTE_USER",0);
    } else {
        error_log("Could not extract user", 0);
    }
} else {
    error_log( "Hcook: nothing here !!", 0);
}
```



- <http://www.rediris.es/app/papi/index.en.html>
- <http://as.maunakea.switch.ch/PAPI/>
- <http://perl.apache.org/docs/1.0/guide/>
- http://www.math.uwaterloo.ca/~oadragoi/CS746G/a1/apache_conceptual_arch.html
- This presentation



- **N x M dependency (AS, PoA's)**
- **Group based assertions about users (and not Attribute based)**
- **Personalized Resources**
- **Transmitted information to Resources**
- **Different assertions about users to different PoA's not solved in this version (no Attribute Policy)**
- **Most authorization is done at the AS (and not at the PoA as needed in our environment)**
- **Some issues should change in the next version**



