

Universal SSPR: A new edge for Self Service Password Reset



Alban Meunier - SmartWave SA
ameunier@smartwavesa.com



Universal

For end-users, dummies, system integrators,
security experts, and you

The logo consists of a central blue circle containing the text 'USSPR' in white, bold, sans-serif font. This circle is surrounded by a white, stylized gear-like border with eight teeth. The entire logo is set against a blue background that features a white, stylized gear-like shape with eight teeth, mirroring the logo's design.

For OpenLDAP, OpenDJ, AD, any LDAP server,
RDBMS, cloud apps, IDM suite, web portals,
Prod + Qua + Dev, and your environment

Why SSPR is a must have

Self-Service Password Reset

- People forget password
- Unlock User account
- Change required after compromised password
- Helpdesk costs
- End user satisfaction
- ...

And because passwords are still widely used

Self Service Password Reset landscape

A crowded world

Google: About 68,800,000 results

Commercial tools

Open source solutions

Identity Management suites

Access Management suites

Application specific

Bespoke implementations

Why reinventing the wheel?

- ❖ Too many small limitations such as
 - Q & A not popular,
 - Multiple user stores (DEV, QUA, PRD, ...)
- ❖ Outdated implementation design
 - Difficult to coexist with BYOD & Domain desktop & VDI
 - Reuse existing components (OTP, captcha, ...)
- ❖ New needs
 - Hybrid infrastructure (Cloud base & on premise user stores)
 - Large set of technologies coexists
 - Audit
 - User Interface is a moving world
 - Many combinations as unlimited requirements
 -





Universal SSPR initiative

Why different

- ❖ inspired from work-field
 - Do what you can with what you have
- ❖ full pluggable design
- ❖ swiss security culture
- ❖ end user experience in mind
- ❖ in open source we trust
 - Someone else can do better than me
 - Share with peers
 - Appreciate any feedback
 - Governance could be light and open



A Quick tour on end user experience

Universal SSPR

Language:

English ▾

Action:

Forgotten password ▾

Identification method:

Security Code via SMS ▾

User name:

Submit



I'm not a robot



reCAPTCHA
Privacy - Terms

English ▾

English

Français

English ▾

Forgotten password ▾

Forgotten password

Change password

Forgotten password

English ▾

Forgotten password ▾

Security Code via SMS ▾

Security Code via SMS

Link via professional email

Google authenticator

A Quick tour on end user experience

Universal SSPR

Language:

Action:

Identification method:

User name:

Submit

Success

Your request has been successfully handled
An email has been send

OK

 I'm not a robot

reCAPTCHA
Privacy - Terms

Error

We are not able to satisfy your request
Please double check parameters and retry or
contact helpdesk: 012 345 67 89

OK

A Quick tour on end user experience

Universal SSPR: Forgotten password

Cible:

Main Corporate Password

User name:

mmouse

Code received:

New password:

Confirm new password:

Submit



I'm not a robot

Success

Your request has been successfully handled
A code has been send by SMS/Mail. Please
proceed to next step

OK

A Quick tour on end user experience

Universal SSPR: Forgotten password

Cible:

Main Corporate Password

User name:

mmouse

Code received:

123456

New password:

●●●●●●

Confirm new password:

●●●●●●

Submit



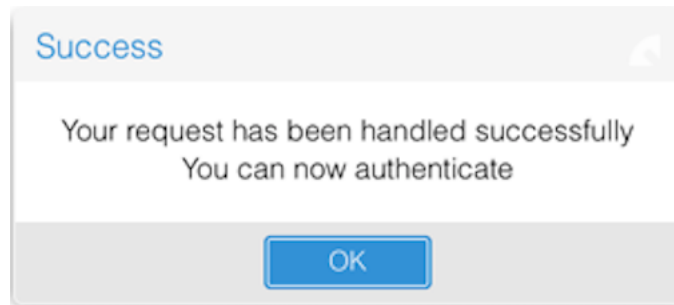
I'm not a robot



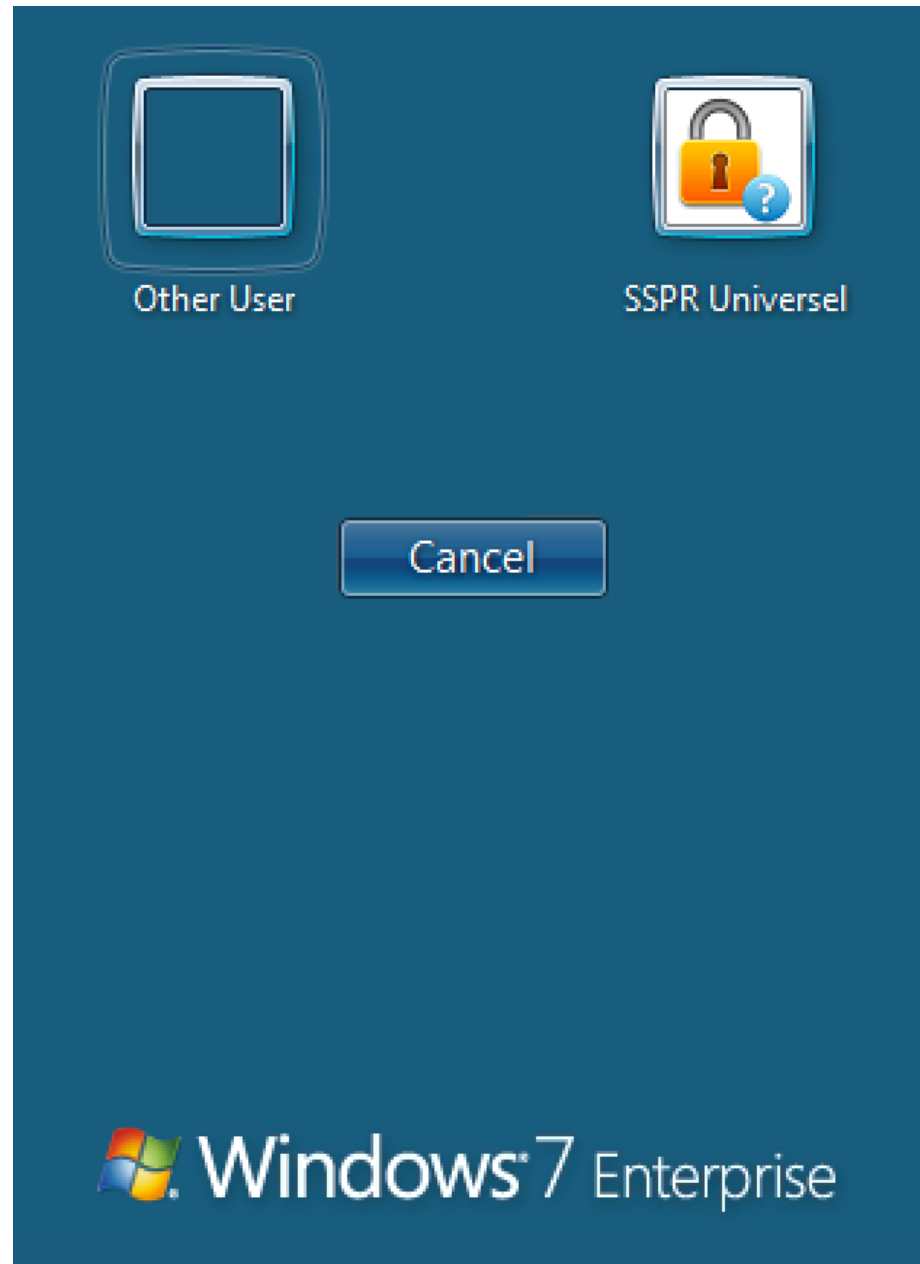
reCAPTCHA
Privacy - Terms



A Quick view



A Quick view of fat client



A Quick view of fat client

SSPR Universel

Universal SSPR


Language: English

Action: Forgotten password

Identification method: Security Code via SMS

User name:

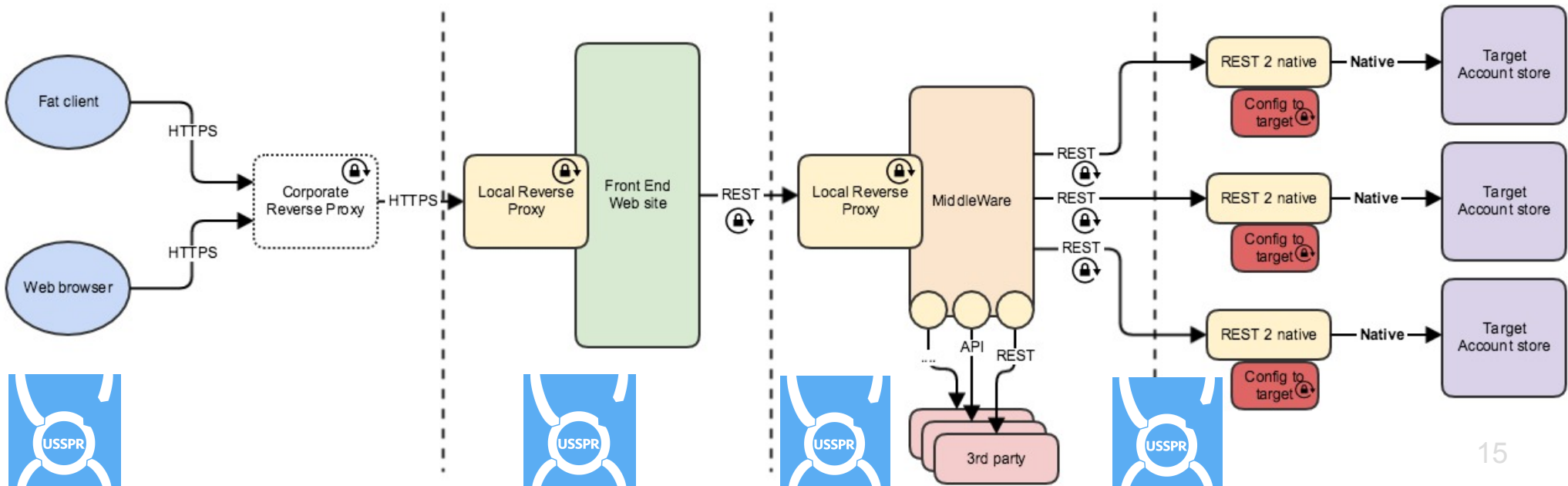
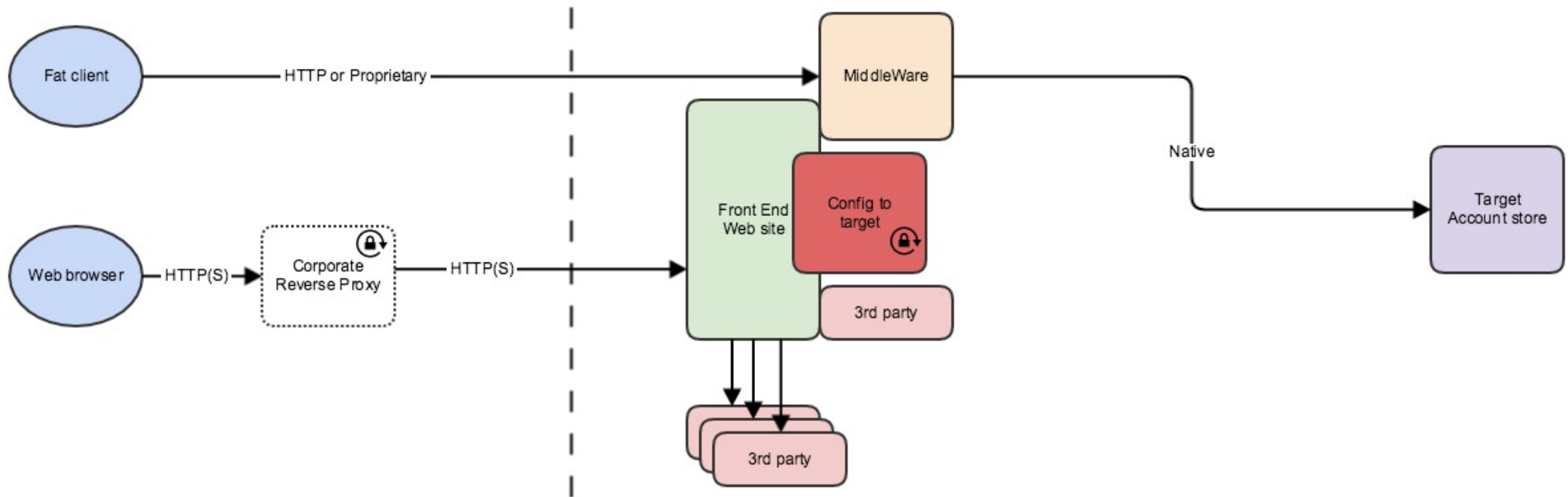
I'm not a robot


reCAPTCHA
[Privacy - Terms](#)

The geek corner









Architecture overview





Components review

End user side

- ❖ Web based
 - Simple UI without technical wording 
- ❖ Fat client
 - Windows Credential provider (based on MS specifications)
 - Restricted mouse & keyboard actions allowed 
 - No local access rights 
 - No internet access and no cross sites 
 - Embedded browser (.NET + config) 
 - SSL required 

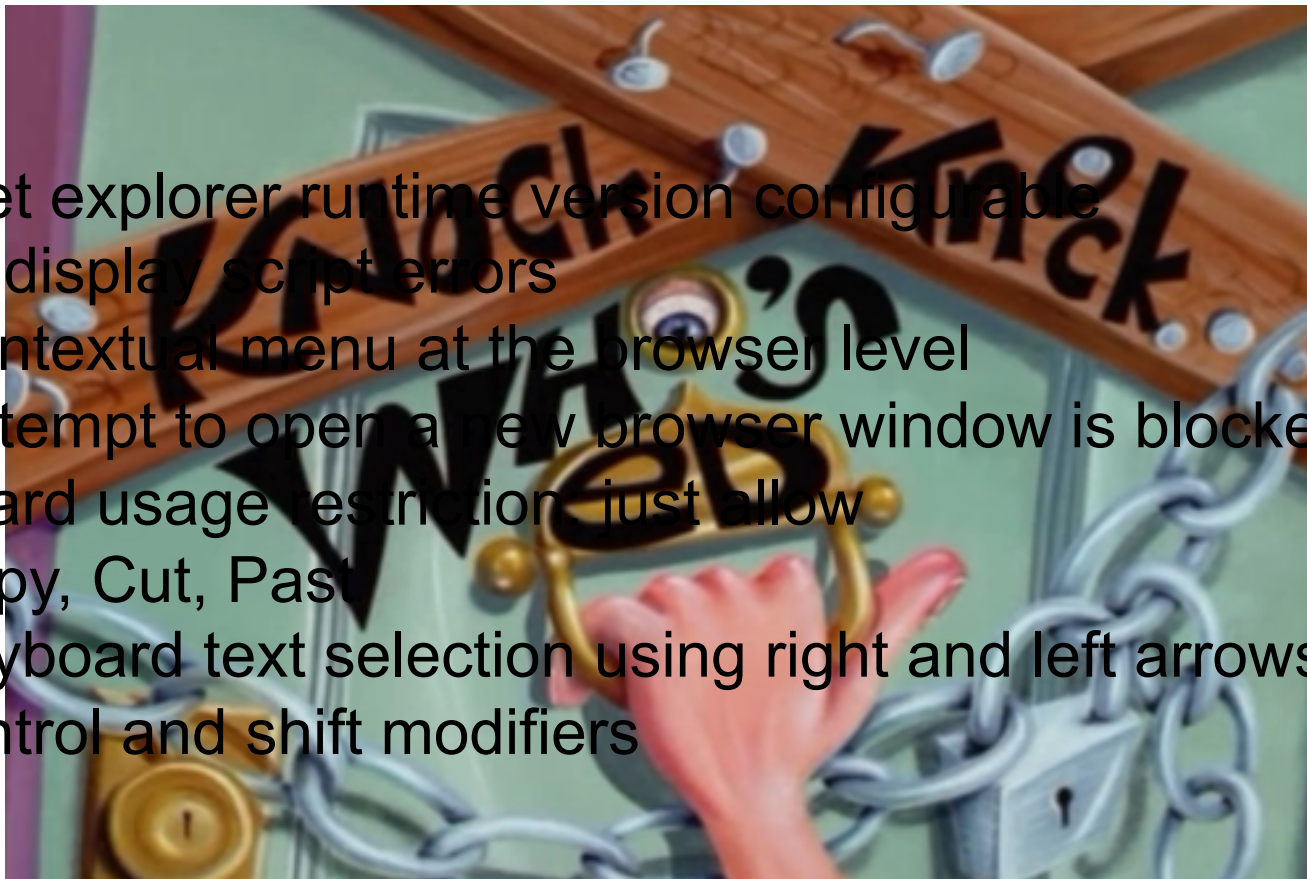


Zoom in on Windows credential provider

HKEY_LOCAL_MACHINE\SOFTWARE\SmartWave\usspr

- BrowserAppPath: C:\Program Files\usspr\usspr.exe
- SsprUrl: <https://myVerySecuredServer.example.com/usspr>







- Internet explorer runtime version configurable
- Never display script errors
- No Contextual menu at the browser level
- Any attempt to open a new browser window is blocked.
- keyboard usage restriction: just allow
 - Copy, Cut, Paste
 - Keyboard text selection using right and left arrows combined to control and shift modifiers





Components review





Front end

- ❖ Run on secured application server (OWASP) 
- ❖ Local Reverse proxy 
- ❖ Minimal design and code 
- ❖ Only 3 Errors and success messages 
- ❖ HTML → REST 
- ❖ “just” a REST consumer
- ❖ No settings about targets 



Components review

Middleware 1

- ❖ Run on secured application server (OWASP) 
- ❖ Local Reverse proxy and API gateway 
- ❖ Business logic
- ❖ Configuration file and no hard code
- ❖ REST calls ONLY 
- ❖ Call 3rd party components
- ❖ Call intermediates to targets but no target config 
- ❖ Audit trail



Middleware Config file

```
"captchaserver":{
  "id":"google",
  "url":"https://www.google.com",
  "path":"/recaptcha/api/siteverify",
  "secret":"fmn6LdJogUTABC007rosqGpfl8cjECuXLzYcsP15EG"
},
...
"identitysources":[
  {
    "id":"WIN_DOMAIN",
    "primary_email":"NO",
    "primary_usrid":"YES",
    "pwd_policy":"01",
    "reset_disabled":"YES",
    "reset_expired":"YES",
    "reset_locked":"YES",
    "rest_url":"https://dc1.int.example.com:8443",
    "rest_path":"/rest2ldap_AD1/users/",
    "source_description":"AD Integration",
    "source_type":"Active Directory",
    "technical_account_id":"sspruser",
    "technical_account_pwd":"Pwd-123!",
    "userfilter_att":"samaccountName"
  },
  {
    "otpserver":{
      "id":"oam13",
      "url":"https://sspriabcore01.cloudapp.net:8040",
      "path":"/oam13/json/users/"
    },
    "logging":{
      "appender.stdout":"org.apache.log4j.Cons
    }
  },
  {
    "pwdpolicies":{
      "max_length":14,
      "min_digits":4,
      "min_length":6,
      "min_lowercase":"","
      "min_specialchars":1,
      "min_uppercase":1,
      "supported_chars":""
    }
  }
]
```



Components review

3rd party components




- ❖ Captcha
- ❖ SMS OTP
- ❖ OATH
- ❖ Mail server
- ❖





Components review

Intermediate(s) to target(s)

- ❖ The only place for targets configuration 
- ❖ REST over HTTPS → native protocol 
- ❖ Located on the most suitable server 
 - middleware server
 - dedicated server
 - target server



Components review

Targets

- ❖ LDAP directory
- ❖ Active directory
- ❖ Data base
- ❖ Identity Management
- ❖ Access management
- ❖ Business API
- ❖ Multi environments
- ❖ ...



Implementation details

Component	Implementation 1	Implementation 2
Client	Windows 7 32 bits Windows 7 64 bits	Windows 8.1 64 bits
Front end	Tomcat ForgeRock OpenIG Sencha ExtJS	Jetty Axway API Gateway AngularJS
Middleware	Tomcat ForgeRock OpenIG Groovy scripts log4j	Jetty Axway API Gateway Axway API policies
3 rd party	Google ReCaptcha Forgerock OpenAM (OTP)	Axway API Gateway
Intermediate to target	ForgeRock Rest2Ldap	ForgeRock Rest2Ldap
Targets	Active Directorie <u>S</u> ForgeRock OpenDJ	Active Directorie <u>S</u> ERP



Current Project status

Some delay to start the community

- ❖ Pilot in progress
- ❖ New requirements
 - Captcha bespoke
 - localization
- ❖ Documentation in draft with missing parts
- ❖ Pending legal & strategic decisions on moving to open-source



Roadmap = Todo list

- ❖ **Fat client**
 - Windows 8
- ❖ **Front end**
 - Localized Sencha apps
 - Other technologies when “nothing” on client side
- ❖ **MiddleWare**
 - Improve Groovy scripts for ForgeRock OpenAM (unlock, ...)
 - Configuration for other API gateway
 - Logger improvement
- ❖ **New features**
 - Change password (and not only reset password)
 - Forgot username



Roadmap = Wish list

Fat client

Windows, 10, OSX, Linux's

3rd party components

- ❖ Verification of a unique code / OTP (REST service)
- ❖ Mail 2 SMS gateway (TBD)
- ❖ Captcha (REST service)
- ❖ Audit/Reporting (TBD)

REST2native gateway

- ❖ REST2LDAP (from various origins)
- ❖ REST2SQL
- ❖ REST2SOAP
- ❖ REST2REST

Packaging

- ❖ Wizard (HowTo, install/config tools)



Contributors

The original contributors are

- ❖ City of Lausanne
- ❖ SmartWave
- ❖ Private Swiss insurance
- ❖ United Nations



All of You are Welcome

- ❖ Personal interest, university projects, corporate program
- ❖ Developers front-end, back-end, middleware
- ❖ Integrators, security officers, testers
- ❖ End users



License



Collaboration spirit: Each user is invited to contribute

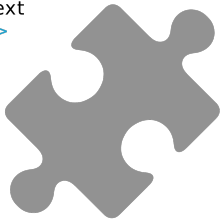
- ❖ No money
- ❖ Intensive & extensive tests and feedback
- ❖ Doc review
- ❖ Code review (security check & fixes, comment, ...)
- ❖ Extensions



Get it

What is provided: a full working solution

```
1 <!Doctype HTML>
2 <html>
3   <head>
4     <meta charset=utf-8>
5     <title>HTML5 example</title>
6   </head>
7   <body>
8     Text
9   </body>
10 </html>
```



- ❖ The core: APIs' definition between front & middleware, configuration file
- ❖ Windows Credential providers (source, exe as example)
- ❖ Example of Web front based on Sencha ExtJS
- ❖ Groovy scripts for ForgeRock OpenIG
- ❖ Configuration file for ForgeRock Rest2LDAP
- ❖ Documentation (architecture, HowTo)
- ❖ Interfaces and config for 3rd party (no limit)



What cannot be provided

- ❖ JRE, JDK
- ❖ Apache Tomcat
- ❖ ForgeRock OpenAM, OpenIG, OpenDJ, Rest2LDAP
- ❖ Microsoft Active Directory
- ❖ ...



Get it

Google group (temporary hosting)

<http://shortlinks.smartwavesa.com/usspr>

Waiting for legal decision
(expected to come soon)



New hosting (source, bin, forum, wiki, wish list, ..),
for smooth collaboration



Conclusion

- ❖ Security, security, security
- ❖ Innovative pluggable design
- ❖ Integration and evolution
- ❖ Extensive collaboration ready
- ❖ Professional services on request (\$)

See you soon on

Mail: sspr@smartwavesa.com

Group: <http://shortlinks.smartwavesa.com/usspr>