Enabling SAML for Service Provider

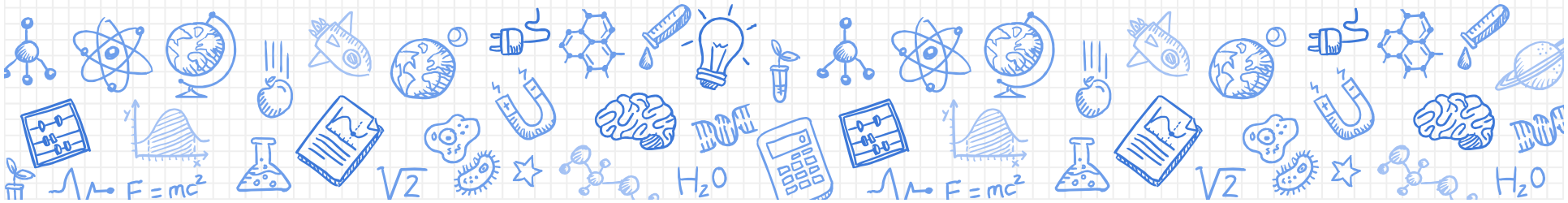
Contact

Jinyong JO and KyoungMin Lee

You can find us at coreen@kreonet.net

Join KAFE as a Service Provider

How to integrate SAML with your Web applications



KAFE(Korean Access FEderation) technically supports Service Providers for SAML integration

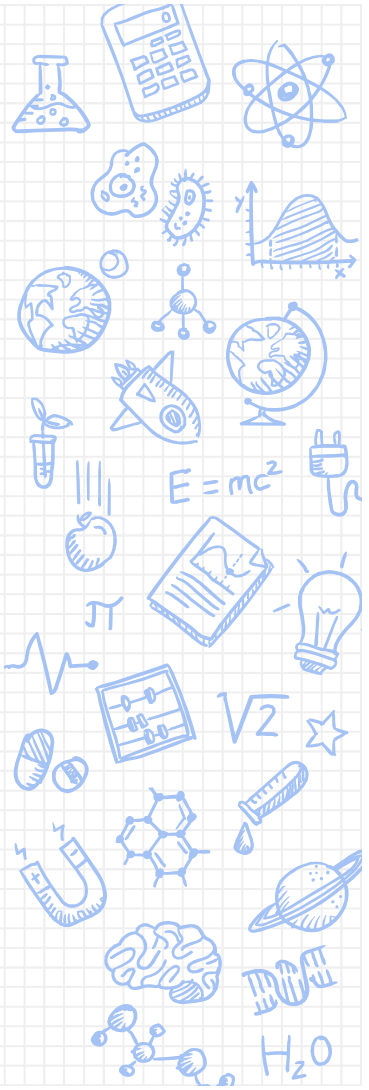
Disclaimer

KISTI는 최대한의 주의를 기울여 작성된 템플릿 코드와 유관 전자문서를 배포하고 있습니다. 그 어떤 경우에도 KISTI 또는 그 구성원은 템플릿 코드와 유관 전자문서 및 그 내용의 오류, 부정확성 혹은 불완전성 및 그 결과에 대해 어떤 법적 책임도 지지 않습니다.

In any case, …

✘ Enabling NTP (Network Time Protocol) is mandatory

- We use time.kriss.re.kr

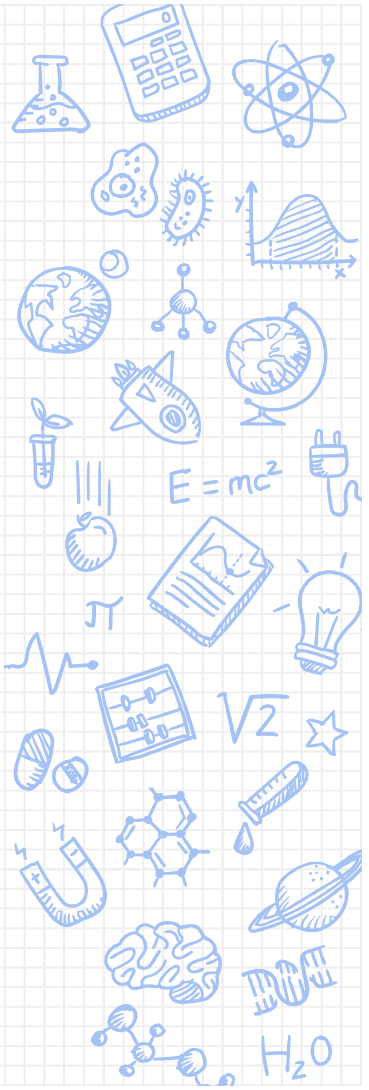


Support for the integration of SAML and Web Applications under…

- ✘ Linux
- ✘ Apache, Tomcat, or Jetty Web Container
- ✘ Almost all Web Programming Language

Windows/IIS support will be, but not now

[July 2016]



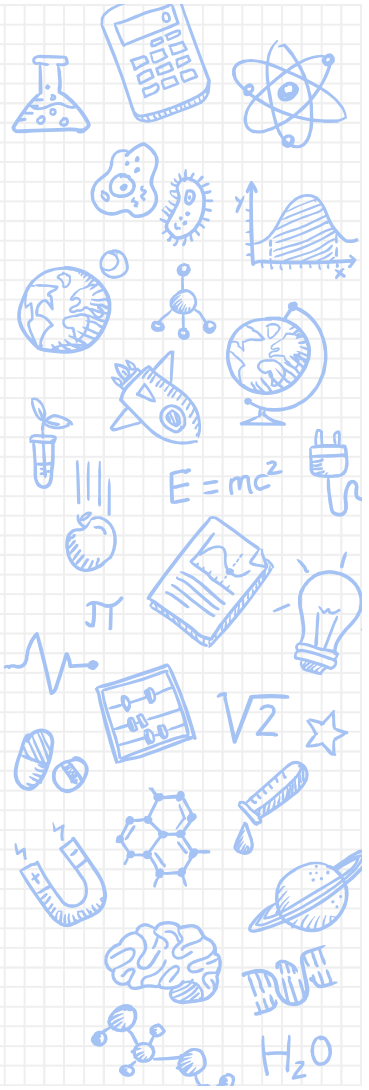
SAML software we recommend

- ✘ simpleSAMLphp
- ✘ Shibboleth [support will be available soon]

Need more verification however possible

- ✘ OIOSAML
- ✘ Spring Security SAML extensions

[July 2016]



Three Ways of SAML integration KAFE supports

✘ Memcached – distributed shared memory

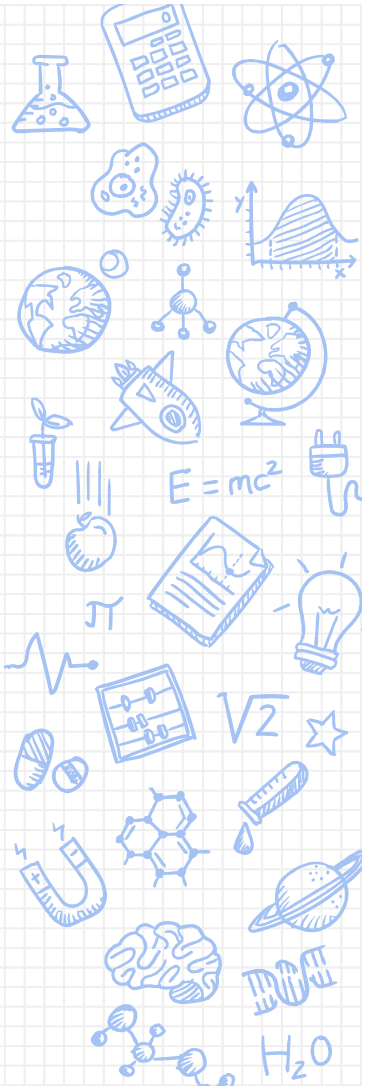
[Use case] Web app is implemented with a different computer lanaguage from SAML software but both are running on the same Web container (e.g., Apache)

✘ Web proxy

[Use case] Web app and SAML software are running over different Web containers (e.g., SAML software on Apache and Web app on Tomcat)

✘ API (Application Programming Interface)

[Use case] Web app and SAML software use the same computer language (e.g., Web app written with PHP and SAML software with PHP as well)



Web Proxy based Integration KAFE supports

[Skip Memcached] Contact coreen@kreonet.net for more information about Memcached

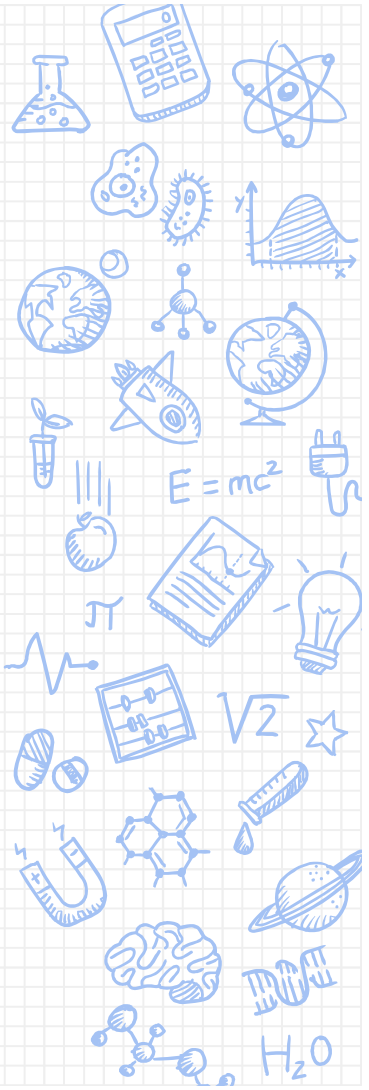
✘ Configuration

- SAML software: simpleSAMLphp running on Apache 2.2 or 2.4
- Web application: Java running on Jetty or Tomcat

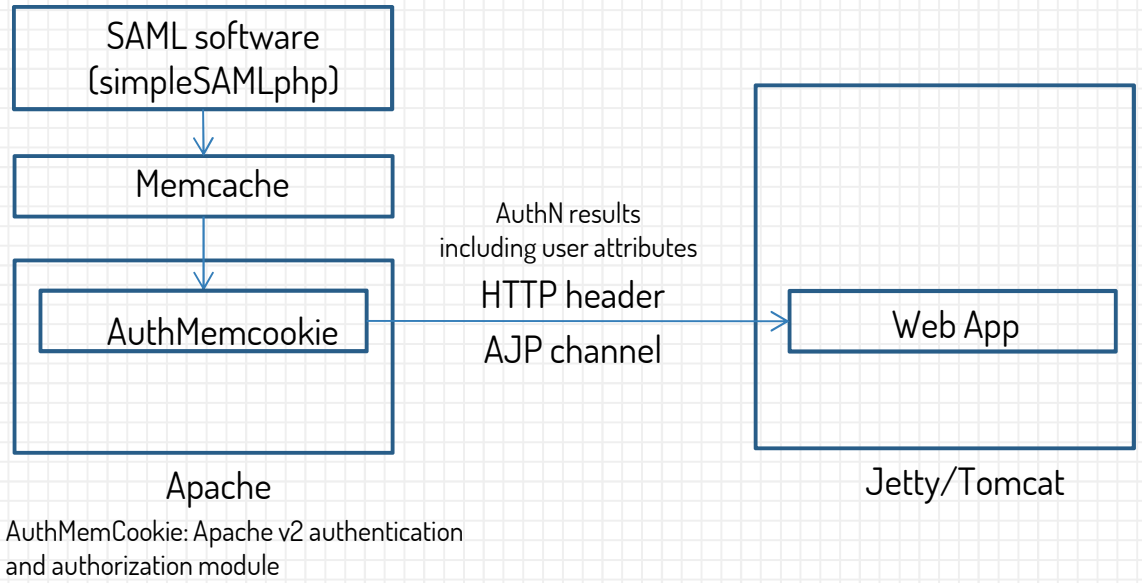
※ All SAML related actions place in Apache

✘ Interface Apache and Jetty/Tomcat

- mod_proxy (Jetty or Tomcat): write Auth Info on HTTP header and pass it to Jetty/Tomcat
- mod_proxy_ajp (Tomcat): use out-band channel to transfer Auth Info.



Web Proxy based Integration KAFE supports (Contd.)



AuthMemCookie: Apache v2 authentication and authorization module

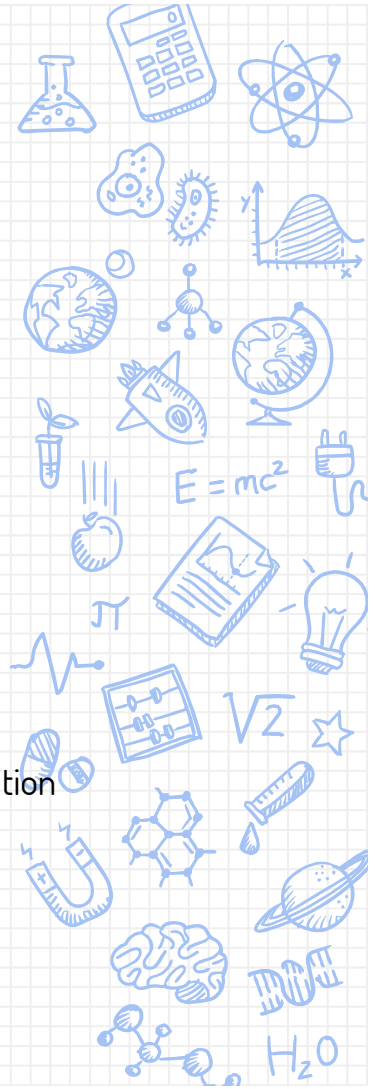
[KAFE provides]
- Installation scripts to automatically comple the lefthand-side software installation and configuration
- Simple example Web App code written with Java (righthand side)
- How-to documents

API KAFE supports

✘ PHP API
✘ Java API

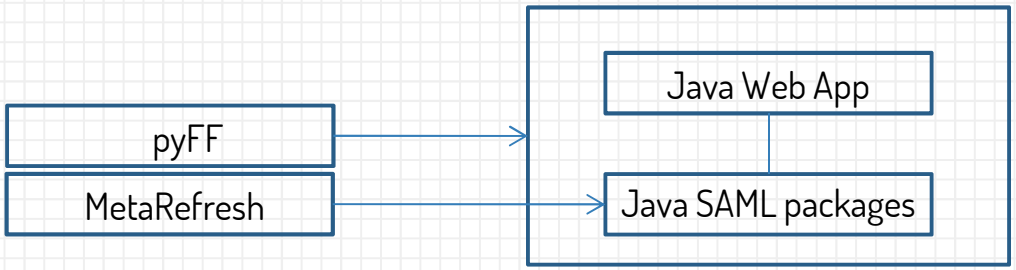
	PHP	Java
Web container	Apache 2.2/2.4	Jetty, Tomcat
SAML software	simpleSAMLphp	OIOSAML, Spring Security

- simpleSAMLphp is available on https://simplesamlphp.org/ . Download and use without modification
- KAFE-version of OIOSAML or Spring Security SAML extensions. Some modifications include
  - Attribute filter for eduPersonTargetedID
  - OID to friendlyName map
  - Discovery service
  - Dynamic metadata-refresh and ETC.

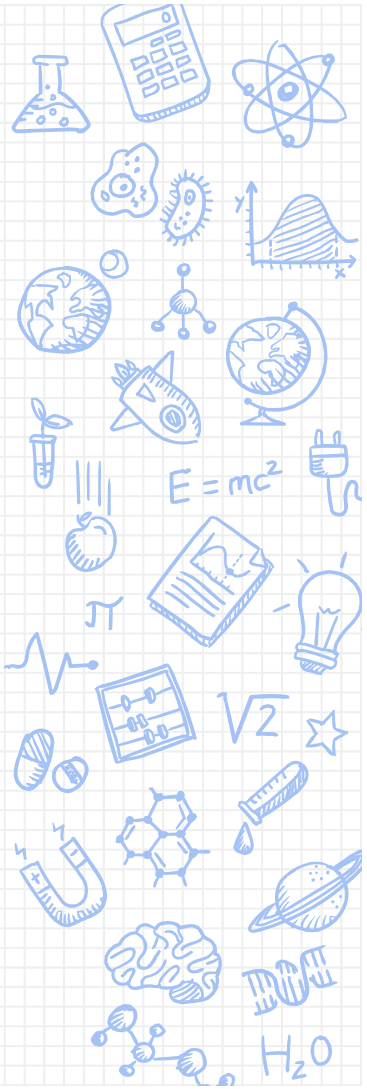


API KAFE supports (Contd.)

✘ Configuration



pyFF: SAML metadata processor,
MetaRefresh is required for OIOSAML

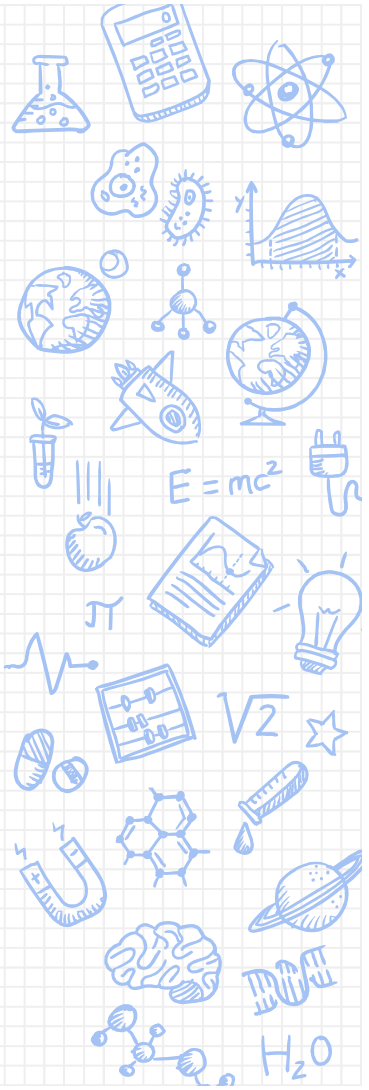


API KAFE supports (Contd.)

✘ Current known limitations of Java API

- can not check SSL certification expireation data
- can not validate metadata signature
- can not validate validUntil [will be resolved]
- [OIOSAML] incompatible HTTP GET parameter (idp=) with general Discovery Service[will be resolved]

[July 2016]

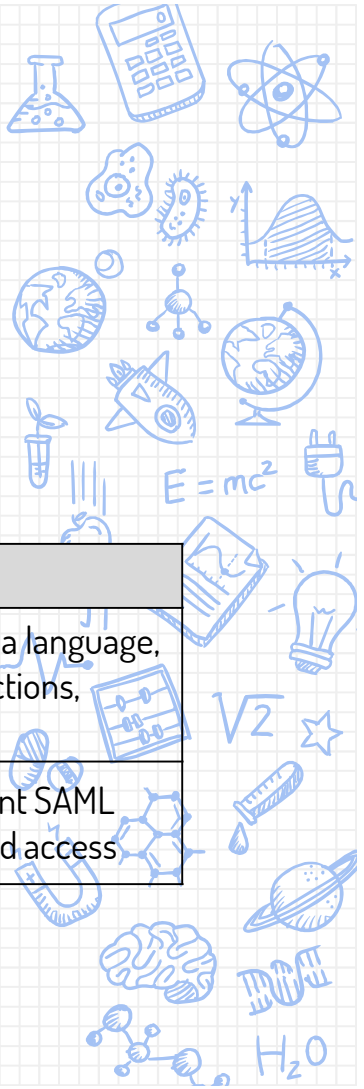


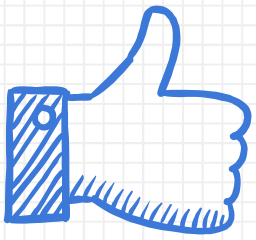
Cases: ONOS network applications (VDN)

✘ Available options

- Web proxy with mod_x proxy
- OIOSAML Java API

	Web proxy	OIOSAML
Pros	Apache takes all for SAML, Use of well-functioned SAML software, Easy to integrate	A single Web container with a language, DIY SAML-related functions, Easy to integrate
Cons	Hold multiple Web containers	Premature and insufficient SAML functions for N:1 federated access





Join KAFE!

Add value to your service

You can find us at

- coreen@kreonet.net
- {jiny92, tsoc}@kisti.re.kr