# Kipper – a Grid bridge to Identity Federation

Andrey Kiryanov



#### Brief

The Kipper client software combines tools and utilities to extend a Web Application to:

- Enable login via federated SSO like eduGAIN
- Retrieve a SAML2 Identity Assertion from SSO
- Transform a SAML2 Identity Assertion into an X.509 proxy certificate with VOMS extensions
- Do it all directly in browser context with JavaScript API

The result: "X.509-free" access to the Grid



## WLCG pilot service

- Goal: give access to WLCG resources using home institute's credentials
   No need for X.509 certificates
- WLCG working group dedicated to Identity Federation
  - CLI (job submission, admin tasks)
  - Web-based (grid portals for job submission, data transfers, etc.)
- Focus on the web-based solution



#### eduGAIN



- Built on existing federations and infrastructures
- CERN participates in eduGAIN via SWITCHaai
- Many NRENs participate in eduGAIN too





#### Access via CERN SSO CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in v	with your CERN account
Reminder: you	nu have agreed to comply with the CERN computing rules
Use crede	entials
Username o	or Email address Password
	Sign in
Rememb	ber Username or Email Address Need password help ?
$\sim$	
Sign in v	with your organization or institution account
* eduGAIN	Enter the name of the organisation you are affiliated with
Related s  Need pass Create/Ch Create/Ch EduGain d Service De Computing Connectio	EduGain_https://shibidp.to.cnr.it/idp/shibboleth EduGain_https://southdowns.ac.uk/oala/metadata EduGain_urn:fi:fer.hubhn02:1.0 EduGain_urn:mace:cnrs.fr:janus.dsi.cnrs.fr EGI EduGain Morgan State University Philadelphia University Swedish National Defence College Educampus Services Ltd
	University of Copenhagen

#### IdF and CERN SSO

- CERN SSO service is based on Microsoft ADFS (Active Directory Federation Services)
- In order to benefit from SSO your Apache web server needs a special plug-in:
  - Shibboleth first solution supported by CERN, widespread, supports all possible standards, not easy to configure
  - Mellon pure SAML2 Service Provider. Minimal configuration, supported by CERN since 2015
     *Kipper supports both natively*



#### SSO log-in process



SAML2 assertion is an XML-formatted signed attribute list, which contains your name, e-mail address, e-groups, etc.



#### **Kipper cornerstones**

- SAML2 to X.509 translation
   STS
- Short-living X.509 certificates
   > IOTA CA
- VO membership
   > VOMS



#### STS

- Security Token Service (STS) consumes SAML2 assertions and produces X.509 credentials in return
  - STS is an implementation of WS-Trust OASIS standard and it speaks SOAP
- STS has been developed in the context of the EMI project and was extended at CERN to support:
  - CERN IOTA CA specific client
  - VOMS DN mapping registration and caching (IOTA DN is an alias to VOMS DN)



#### STS integration in a Web Application





#### IOTA CA

- IOTA CA (Identifier-Only Trust Assurance Certification Authority) issues short-living (days) X.509 certificates
- First implementation was issuing certificates to any STS client (provided that it had a valid assertion)
- Now STS can ask to sign certificates only for users registered in the configured VOMS
  - Handy if you need a restricted set of eduGAIN
     members that would get a valid certificate



### **DN** uniqueness

- IOTA CA should use an eduGAIN persistent identifier attribute to return a unique DN
- Which attribute(s) can be considered persistent and unique in eduGAIN?
  - *eduPersonPrincipalName* is considered unique in theory but it can be reassigned according to local policy
  - Only Identity Providers that secure unique eduPersonPrincipalName will be enabled in STS



#### CERN LCG IOTA CA

- A document containing all the details for the new CA at CERN has been prepared in 2015 by CERN IT IdF Team with help from us
- The document went through the review process of EUGridPMA and was accepted
- CERN LCG IOTA CA is included in IGTF Trusted
   Anchor Distribution since version 1.72
  - Deployed on virtually all WLCG sites now
  - It should "just work" for you



#### **Open issues**

- The new IOTA DN is associated to the already existing one in VOMS, but the grid middleware is not aware of this alias
  - Two different users (not always an issue since proper VOMS extensions are included in the certificate)
- Dedicated STS instance per each WebApp+VO combination
  - VOMS DN mapping and checks
  - WebApp and STS need to consume the same SAML2 assertion



#### Use cases

- What kind of web applications could benefit from Kipper?
  - All kinds of portals that need to talk directly to Grid resources with X.509 authentication
  - Data and workload management interfaces
- What are the benefits?
  - Clear distinction between users (no catch-all robot proxies)
  - No need to maintain App-specific user database
  - Security, VOMS support
- What needs to be changed in the WebApp?
  - Backend web server needs to be Apache on Linux (no IIS yet)
  - Server side needs to accept user proxies from browser via specific delegation mechanism
  - A dedicated instance of STS needs to be deployed



### Ongoing work

- CERN is developing a portal to enable eduGAIN members that are also members of LHC VOs to get a proxy certificate out of their eduGAIN credentials
- There's an ongoing integration of ATLAS Panda Monitor with SSO which will allow then exploiting Kipper to transparently access job/monitoring log files stored on Grid storage elements



#### What is WebFTS?

- https://webfts.cern.ch
- Web-based tool to transfer files between Grid/cloud storages
- Modular protocol support
  - gsiftp, http/dav, xroot and srm
  - Cloud extensions: Dropbox





#### WebFTS pilot

🔍 🥠 WebFTS - Simplifying pov	+ ×									
A https://webfts-dev.cem.ch/submi	t.php#				7 C	Q, Search		合 自	+	ń
e not providing a valid user certif	icate					You	are authenticated	i as Andrea Man	el Ge	Le
					You	r current prox	y is valid for 11 ho	urs for the VO bi	face -	
WebFTS (Beta v	ersion) Sympl	ifying pow	er							
ft Home			≣ My jobs	<> Submit a transfer						
CON Ordel SE					CON Orid SE					
Grid Storage B	emont		•	<	Grid Stores	e Element				
https://xfsra04a04.cern.ch/dpm/cern.ch/home/dteam/ Load				jsiftp://bdsra04a04.cern.ch/dpm/cern.ch/home/bitface+  Load						
Select All None	C Refresh Show	filters		Overwrite Files	Select All None	C Refrest	h Show filters			
Name	Mode	Date	Gine	Compare	biama	Mode	Date	Qise		
0	Mode	LARIE	OIZE		0	Mode	Late	OIZE		
00martin	drwxrwxr-x	25 Nov	-	LFC Registration	Event.root	-rw-rw-r	26 Jan 11:10	936.2 kB		
<b>=</b> 10016	descence.v	10:46	_	II0://	services 1	-rw-rw-r	26 Jan 14:43	19.1 kB		
- 10010	GIWAIWAI-A	16:26	-		0 File(s) Selected					
<b>1</b> 0143	drwxrwxr-x	05 Dec 17:29	-							
10155	drwxrwxr-x	03 Nov 11:01								
<b>a</b> 10215	drwxrwxr-x	20 May 14:57								
<b>i</b> 10265	drwxrwxr-x	17 Oct 13:31								
10487	drwxrwxr-x	10 Oct 13:54								



#### "X.509-free" access

- X.509 delegation is needed to let WebFTS access the Grid resources on user's behalf
  - User needs to make his private key available to the browser
  - Browser keystore is not accessible via JavaScript API
- A first prototype integrated with STS and IOTA CA
   was implemented at the end of 2014
  - WebFTS-specific solution, no Kipper yet
  - Initially STS returned a plain certificate then delegated to FTS3 which was in charge of requesting VOMS extensions



#### Segregation of Kipper from WebFTS

- Detached codebase of STS and Kipper
- WebFTS uses Kipper as a library
- Following the changes in STS with the generation of VO-specific certificates, we have adapted WebFTS (and Kipper) to use proxy certificates and delegate them to FTS3
  - Move to RFC proxy generation was needed
  - Still both scenarios are supported
- WebFTS is the first technology demonstrator



#### Conclusions

- Kipper enables Federated Identity Web-based access to WLCG resources
- IdF-enabled WebFTS is a working prototype (available only inside CERN so far)
  - ATLAS has kindly agreed to provide its VOMS for testing purposes
  - CERN LCG IOTA CA is globally deployed on WLCG sites
- This is an important step towards "X.509-free" access to Grid resources



#### Acknowledgements

Andrea Manzi Oliver Keeble Henri Mikkonen Romain Wartel Emmanuel Ormancey

This work was funded in part by the Russian Ministry of Education and Science under contract №14.Z50.31.0024



#### References

https://gitlab.cern.ch/sts
 STS and Kipper sources

https://cafiles.cern.ch/cafiles/
 CERN LCG IOTA CA certificates and documents



## Thank you!

