Minutes of combined *security* and *data* EMI Group

Participants : Vincenzo Ciaschini, Paul Millar, Daniel Kouril, Oscar Koeroo, Joni Hahkala, Mischa Salle, Patrick

Minutes have been provided by Vincenzo :

Purpose of the discussion

What needs to be done on our components to migrate from GSI to SSL and what strategy should we choose to do it ?

Agreements :

- Agreed to use different ports for GSI and SSL interfaces
- Using Proxies with SSL. There are many current solutions: Joni's, Oscar's, Vincenzo's. Any of them should work.
- If delegation is needed, it should be driven by the server, not by the client.

Actions:

- *Everyone*: Discuss the above within their own group.
- *Vincenzo*: Get info and feedback from the WMS guys, who were absent today.
- *Paul+Patrick*: Contact Alex Sim (American SRM expert) and CASTOR people to ensure synchronization among different implementations
- *Vincenzo*: Set up a phone conference in 2 weeks time (around end of month) to continue discussion also with the missing representatives.

Final remarks

What should be prepared for the phone conf: people who have been present here should be report on their internal discussion, and especially clarify the missing parts, e.g: Which delegation implementation to use? If other problems are found, tham they should also be discussed there.

People which was not present today should instead be prepared to discuss their own problems and strategies.

Detailed discussion as rembered by Vincenzo and doublechecked with all participants :

Vincenzo: For voms the job is already done. It uses the callback support from OpenSSL to detect the wrapping done by GSI on SSL and remove it, passing clean SSL messages to the rest of the OpenSSL stack.

Daniel: For our software, we use the globus library via its GSS calls, but we set the plain SSL bit from the start, so we do not need to migrate since we are already speaking clean SSL. Additionally, we like the GSS support in globus because for example it meshes well with the Kerberos-based authn in our organization.

Paul: We could provide plain SSL interfaces on a separate port. This would permit easy compatibility with legacy clients that try to speak GSI.

Oscar: We too are already speaking plain SSL + support for proxies in glexec. However, we do not support delegation because we do not need it.

Daniel: We also do not support delegation.

Vincenzo: Voms too does not support delegation, because we do not need it.

Patrick: On the other hand we need delegation, because it is necessary for some SRM operations like SRM copy

Daniel: You could use gridsite, which does support delegation as an additional service

Vincenzo + Joni: There is also a dedicated service on gLite exactly to provide delegation.

Joni: On the delegation web service port type, there was work to make the glite-gridsite and GT versions compatible, and in high level they should be. But in details the globus one relies a lot on the WS-RF etc. But delegation works the same way, the principle is simple, but details differ.

Paul: I remember there is also a firefox plugin to do it. It is not acceptable as a solution, but it would be interesting to see how it works.

Paul: I think we could use gridsite without problems

Joni: Our alternative implementations are however incompatible with the one in globus. Delegation will work in a different way.

Mischa: That would be nice, because we now have a kind of vendor lock on globus exactly because of its implementation of delegation. It would be nice to remove this lock.

Oscar: Delegation implies support for proxies. Before working on SCAS I did it via OpenSSL callbacks, and other on this table did it too.

Paul: Indeed, we need support for proxies.

Joni: Trustmanager for java supports that. Which container do you need?

Paul: We are using tomcat, but we are moving away from it, and prefer Jetty.

Joni: Trustmanager supports both. Also, we do not rely on globus libraries for it.

Paul: I think we already use jglobus, but I am not sure and should check.

Paul: On the other hand, jglobus has switch to change from gsi to ssl. This would seem the simplest solution.

Oscar: We should however remove the vendor lock on the protocol vendor lock. We could support delegation in the secure AuthN library.

Paul: We need delegation for third party copies, where it is always necessary. However, there is no need to always do delegation at the start, and would prefer to do it only if needed, with a process started by the server. Additionally, this is strictly speaking not a part of SRM since SRM is agnostic on how it is implemented.

Patrick: I concur: we may need delegation down the line depending on the type of operation, but we do not need to always do it at the start of a connection.

Paul: We also do not need to be backwards compatible with previous version. If we do this on a different port, we may support it via new clients while still supporting older clients, since we also cannot mandate worldwide upgrades.

Joni: How about the clients? How will they know when to delegate and when not to delegate.

Paul: Right now, dcache alway delegates. I do not know what lcg does. However, I would prefer that logic to

be in the server.

Joni: FTS know when it is needed and when it is not.

Patrick: FTS has one implementation. dCache has several clients which do not know when it is needed or not.

Paul: It is not so simple for clients to always know when it is needed for us. This is why the decision should be done by the server part of the architecture.

Paul: There is interest in the SRM community in moving to SSL. If we can show some speed increase or at least no hits we can push the community in this direction.

?: But the vendor SSL support do not support proxies.

Oscar: This is not true. We at NIKHEF managed to convince vendor devices to support RFC 3280 proxies.

Vincenzo: Would it be reasonable to say that if we succeed in moving to SSL only we could just use our certificates?

Mischa: Not really, for glexec, for example, we need proxies. But we are indeed doing too many delegation we do not really need, and we should cut down on those.

Paul: I think I could also go to the SRM tables and push a way for the server to hint that it would like delegation.

Oscar: You could also just hack the return message to write it there.

Paul: Yeah, but for compatibility reason we would prefer a smoother way to do that.

Vincenzo: However, I think that if you went to the SRM guys with a working prototype you would have a much stronger argument.

Paul: Agreed.

Oscar: Anyways, I think that if the major implementations were convinced to go this way, the other ones would just follow.

Paul: Does the delegation service has an URI we could just return?

WHO ANSWERED?

Joni: For trustmanger the gsi migration is not relevant as it has always worked only with plain ssl, gsi is not supported.

Vincenzo: Ok, what I got from all of this is the following: Among the services represented here, SRM implementations, and specifically dCache, are the ones that requires most work. The following strategy, which was also mentioned beforehand, seems reasonable to me: As a first step, a new port is published that is SSL only and only supports the type of requests that do not need delegation. Requests that may need delegation will go through the existing GSI port. New versions of the clients will use one or the other port depending on the request.

As a second step, support for an external delegation service will be added, and the it will allow all requests from new clients to go through the SSL port. The GSI port will however remain until legacy clients will need to be supported.

Do you believe the above strategy is reasonable?

Paul: It should work.

This just in: Paul confirms that they use jglobus and that switching the SSL bit there would be the easiest path.

-- PatrickFuhrmann - 16-Sep-2010

This topic: EMI > EmiDataMinutes20100916
Topic revision: r3 - 2010-09-17 - PatrickFuhrmann