BEEM - Android XMPP - Support #479

Two way authentication using SSL

01/19/2013 01:19 PM - Yakub Moriswala

Status:	Feedback	**Start date:**	01/19/2013
Priority:	Normal	**Due date:**	
Assignee:	Nikita Kozlov	**% Done:**	0%
Category:	XMPP	**Estimated time:**	0.00 hour
Target version:			

Description

Hi,

I want to implement two way authentication using SSL. I checked the server authentication working good but now I want to authenticate users using client certificates.

Is there any implementation available for client authentication in Beem ?

Any help would be appriciated.

Thanks,
Yakub Moriswala

History

#1 - 01/19/2013 01:22 PM - Yakub Moriswala

[+additionally]

We are using Openfire XMPP server.

#2 - 01/24/2013 11:59 PM - Frédéric Barthéléry

- Category changed from XMPP-Jingle to XMPP

- Status changed from New to Feedback

- Priority changed from High to Normal

- Target version deleted (Dev)

SSL mutual authentication is set by the standard java mechanism to create SSL sockets. This is a starting point to implement it in Beem.
In the BeemService class, we use a custom SSLContext and set it in the initMemorizingTrustManager(). You have to configure this SSLContext to do mutual SSL authentication.

Then according to http://tools.ietf.org/html/rfc6120 and http://xmpp.org/extensions/xep-0178.html
the server should present the EXTERNAL SASL mechanism. This mechanism is currently not supported in aSmack, but it is pretty simple to handle it.
An implementation already exist in Smack but was disabled in aSmack.

These type of questions should be sent on the mailing list for more broader audience

#3 - 01/28/2013 07:41 AM - Yakub Moriswala

Frédéric Barthéléry wrote:

> SSL mutual authentication is set by the standard java mechanism to create SSL sockets. This is a starting point to implement it in Beem.
> In the BeemService class, we use a custom SSLContext and set it in the initMemorizingTrustManager(). You have to configure this SSLContext to do mutual SSL authentication.
>
> Then according to http://tools.ietf.org/html/rfc6120 and http://xmpp.org/extensions/xep-0178.html
> the server should present the EXTERNAL SASL mechanism. This mechanism is currently not supported in aSmack, but it is pretty simple to handle it. An implementation already exist in Smack but was disabled in aSmack.
>
> These type of questions should be sent on the mailing list for more broader audience

Thanks for the initial startup!!!