CS-6910: Advanced Computer and Information Security (ACIS) FALL – 2006

Trusted Group Membership Service for JXTA

By

Durga Koka

Department of Computer Science

Western Michigan University

Instructor: Prof. Leszek T. Lilien

Topics covered…..

- What is JXTA
- Abstractions in JXTA
- Trusted groups
- Membership policy
- One side and two side authentication in JXTA
- Trusted group membership service…in OPPNETS.

What is JXTA (JUXTapose)

- JXTA technology is a set of open protocols that allow any connected device on the network ranging from cell phones and wireless PDAs to PCs and servers to communicate.
- Binding: It can be ported on any language.

Abstractions employed by JXTA

- Uniform-peer addressing
- Peer groups
- Advertisements
- Resolver
- pipes

JXTA virtual network

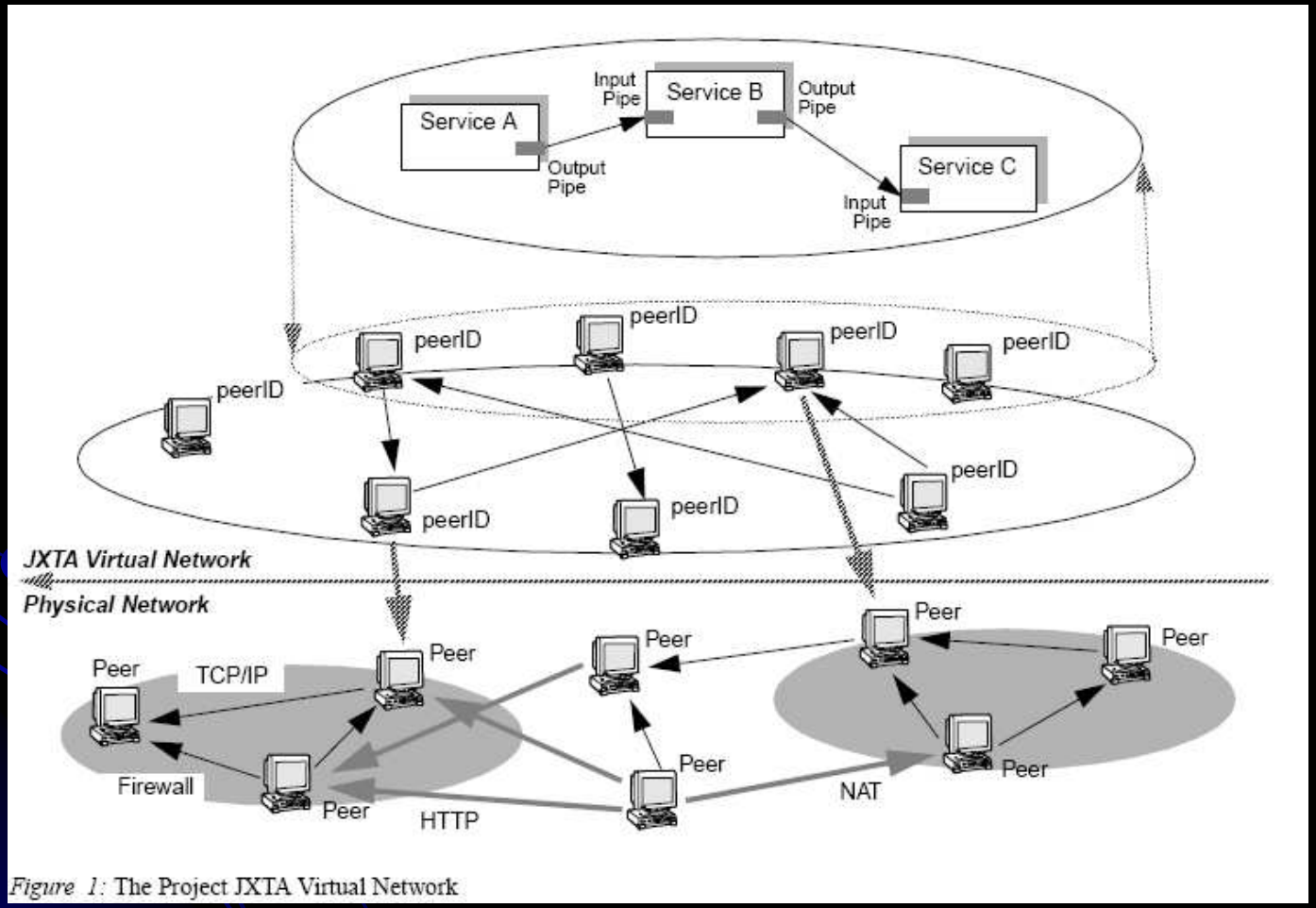


Figure 1: The Project JXTA Virtual Network

Authentication in JXTA

- Group access authentication for JXTA
  - passwords
  - Null authentication
  - certificates and PKI

Trusted groups and membership service

- World peer group
- Net-peer group

- JXTA uses Advertisements to publish the network resources.

A peer has to establishes the identity within a peer group to join a group.

Peer groups will have Membership policies.

Contd…

- The membership policy establishes a temporary identity for the peer.
- Once the peer’s identity is proved, the policy provides the peer with credentials.

Contd….

- Two steps involved in establishing identity to a peer in a peer group:

1) applying for membership:

The peer provides the membership service an initial credential to establish the identity of this peer.

The membership service returns the authenticator object.

The peer group instance is assumed to know how to interact with the authenticator object

Contd…

2) Joining a peer group

After successful authentication, the membership service gives a credential to the peer and allowing that to join the peer.

3) Resigning from a peer group.

- Authentication credentials are used by the JXTAMembershipService as the basis for applications for peer group membership.

One sided authentication

- The peer invokes membershipService's apply method
- peer group obtains certificate from LDAP.
- The peer signs the data with its private key and returns back the data invoking the join method.
- peer group authenticate the peer using the data and its public key.

Two sided authentication

- The peer generates the stochastic data signed by the peer groups private key.
- The authentication of the peer group is made using peer group public key.

Architecture of Trusted Membership service

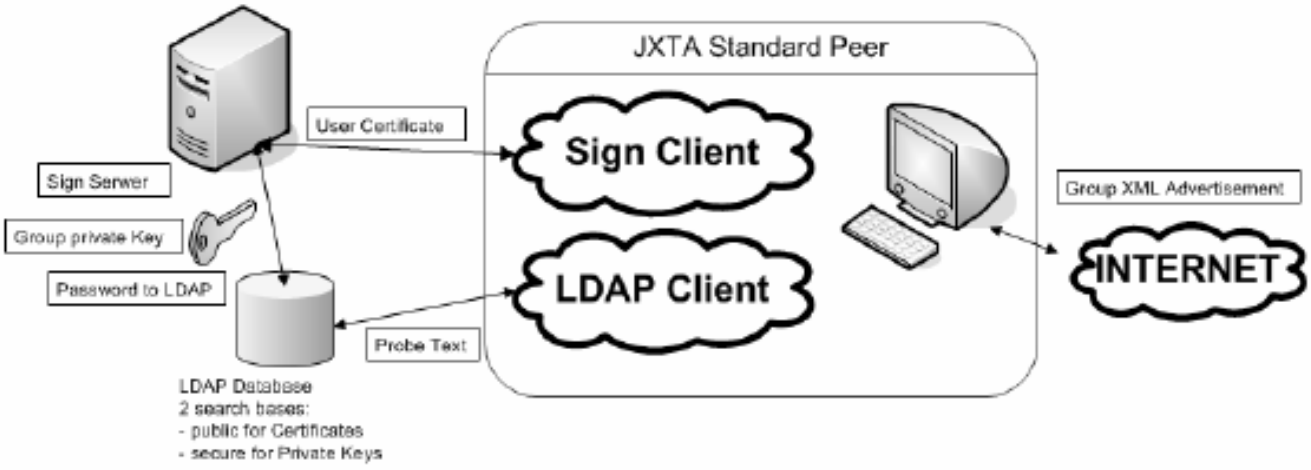


Fig. 1. Architecture of Trusted Membership Service implementation

Implementation details

- Trusted JXTA Group Advertisement

<?xml version=„1.0”?>
<!DOCTYPE jxta:PGA>
<jxta:PGA xmlns:jxta=„http://jxta.org”>
<GID>urn:jxta:uuid-8A12B3AEC66E47BAB739999684D1705302</GID>
<MSID>urn:jxta:uuid-DEADBEEFDEAFBABAFEEDBABE000000016FC5C1F3F7434F658A1C8C6CADFC43DB06</MSID>
<Name>VoteGroup</Name>
<Desc>Peer Group using Certificate Authentication</Desc>
<Svc>
<MCID>urn:jxta:uuid-DEADBEEFDEAFBABAFEEDBABE00000000505</MCID>
<Parm>
<GroupDNName>EMAILADDRESS=CertGroup1@agh.edu.pl, zN=CertGroup1, OU=ICS, O=AGH, L=Krakow, ST=Malopolska, C=PL</GroupDNName>
<LdapServerPort>389</LdapServerPort>
<LdapServerHost>192.168.2.4</LdapServerHost>
<LdapServerSearchBase>dc=PP</LdapServerSearchBase>
<SignServerPort>500</SignServerPort>
</Parm>
</Svc>
</jxta:PGA>

Contd..

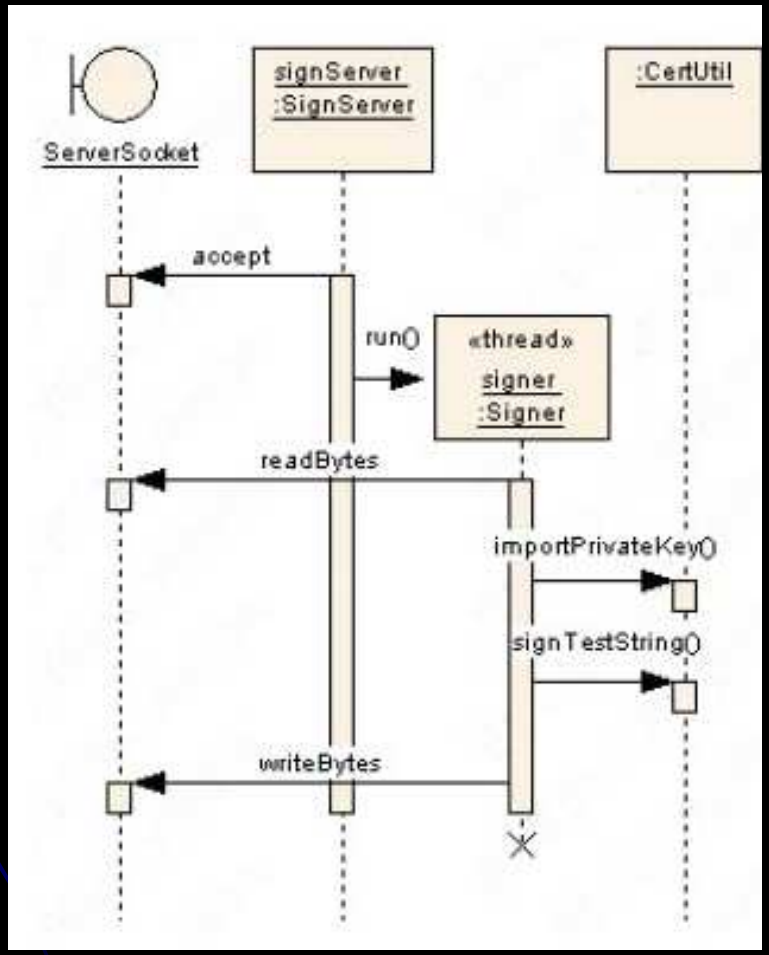
- LDAP configuration

  X509 certificate attribute are created for certificates to be in PEM or DER formats.

- Sign Server

  It is an independent application which performs a group authentication.

- The activity of the Sign Server



- *One side authentication Sequence*

  - The group uses the CertMembershipService class to perform authentication services.
  - The peer invokes the join method in this class.
  - The apply method sends back to the peer, an CertAuthenticator object
  - The peer invokes isReadyForJoin method by giving its certificate and data signed with private key.
  - The group verifies the peer's identity.

Two sided authentication sequence

-- While calling the CertAuthenticator object, setAuthGroupVerificationString method should be used to set the information to be signed by a group

-- At the end, verifying group must be added using the Sign Server connection.

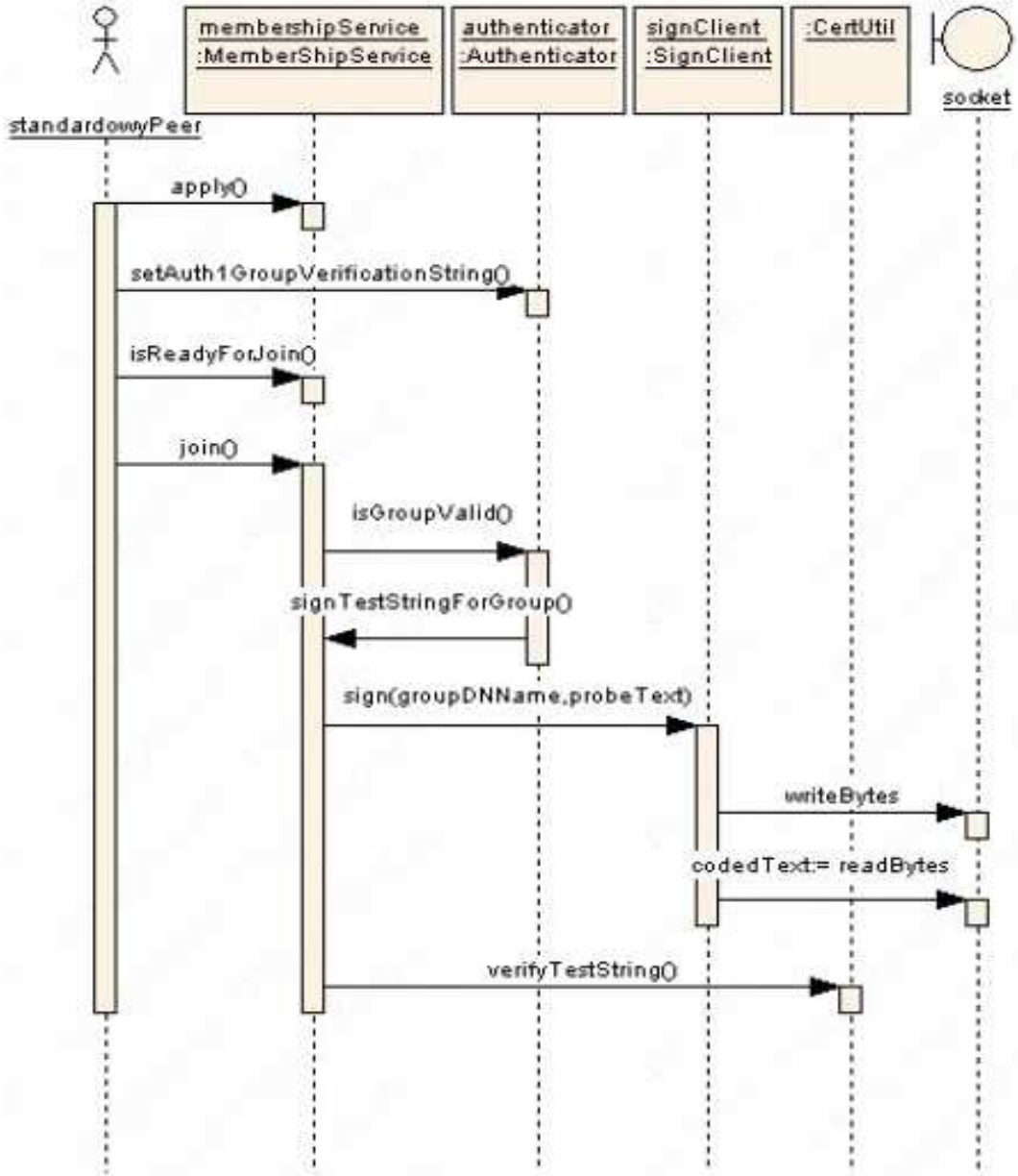


Fig. 4. Diagram of authenticator operation sequence in case of the two-sided authentication

In OPPNETS

- Trusted group membership service can be implemented in OPPNETS.
- When a new helper node wants to join a group, authentication is done from both one side and two side.
- After successful authentication, the helper node is given a certificate and allowed to join the oppnet group.

Conclusion

- This trusted membership service is fully complaint to JXTA.
- The problem of private key secure protection which is a problem for peers and peer groups is addressed by encoding the keys and a proxy object for group.

References

[1] Trusted Group Membership Service for JXTA

http://www.springerlink.com/content

[2] JXTA Project

http://www.jxta.org

[3] JXTA programming guide

http://www.jxta.org/docs/JxtaProgGuide_v2.3.pdf

[4] PKI security for JXTA

http://www.jxta.org/docs/pki-security-for-jxta.pdf