1. Motivation

Security is of vital importance in distributed applications. Microsoft latest development environment offers *remoting* and *web services* for distributed application development using http channel for remote object referencing and serialization in XML. Our project will demonstrate application of Windows CryptoAPI that’s extended to .NET to provide *Authentication* and *Data Integrity* in client server architecture.

2. Development Phases

2.1 Phase 1: Symmetric/Asymmetric Key encryption on local system.

(a) CryptoAPI implements RC2, DES, TrippleDES symmetric key algorithms. Rijndael algorithm is also available as .NET managed code. Using any of the available algorithms, this phase will demonstrate generation of strong symmetric key in a GUI based application for text message encryption and decryption.

(b) Second sub phase will demonstrate the usage of Asymmetric Key by either using RSA or DSA algorithm. Key pair will be generated and stream ciphering will be used to encrypt and decrypt message stream in a simple GUI based application.

2.2 Phase 2: Digital Envelop to establish Secure Communication in distributed arch.

Based on SSL model, this phase of demonstration will provide secure communication channel for client-server system. Asymmetric key pair will be used for authentication whereas symmetric key will be generated by remote server at runtime and passed back to client for communication. This key will act as session key and all further communication will be based on symmetric key cryptography.

For asymmetric authentication, RSA will be used and for session key DES crypto-algorithm.

2.3 Phase 3: Digital Signatures in distributed architecture

Message digest will be created using the standard MD5. This message digest will be encrypted using asymmetric key on client side. Message will be passed using *remoting* RPC and server will verify signed message by comparing its hash.
2. Phases Deliverable Dates

Deliverable after each phase is software application (accompanied with demonstration).

Monday 6, January 2003
*Phase 1: Symmetric/Asymmetric Key encryption on local system.*

Monday 20, January 2003
*Phase 2: Digital Envelop to establish Secure Communication in distributed arch.*

Monday 3, February 2003
*Phase 3: Digital Signatures in distributed architecture*

3. Architecture

3.1 Basic Sequence Diagram for *Phase 2:*

<table>
<thead>
<tr>
<th>Client</th>
<th>Server</th>
</tr>
</thead>
</table>

- Generate key pair
- Exchange public key
- SendSessionKey(EncSPkey(skey))
- Decrypt
- MessageExchange(Encskey(msg))
3.2 Basic Sequence Diagram for Phase 3:

3.3 Technologies:

3.2.1 Base: .NET CLR, CryptoAPI, CryptoStream, CryptoServiceProvider

3.2.2 Comm.: SOAP, .NET Remoting, XML Parser

3.2.3 OS: Windows 2000 or higher on Workstations and Servers

4. References

*Simon Robinson and Steve Danielson:* Professional C#

*Microsoft Corporation:* Visual Studio .NET Combined Help Collection CD

*Microsoft Corporation:* Microsoft Developers Network MSDN online
http://www.microsoft.com/msdn

*Vijay Kumar:* Understanding .NET Security

*Gowri Paramasivam:* Cryptography in Microsoft.NET

*Don Kiely:* Security in .NET