Network Knowledge Call #3

January 13th, 2004

Outline

- Node Building Resources Review
- Mentoring Meeting Announcement/Reminder
- Flow Deployment Resources Review
- Network Security
  - Online Demonstration at the end of the call

Resources for Node Builders

- Network Help Desk
- Demonstrated Node Configurations (DNCs)
- Testing Tools
  - https://test.epacdxnode.net/test/
- Exchange Network Discussion Board
- Guidance and Technical Documents
- Node Mentoring Group

Network Help Desk

The CDX/Network Help Desk is available for any Network or Node building question.

By Telephone:

Call our toll-free line between the hours of 8:00 am and 6:00 pm (Eastern) at 888-890-1995 (Select Option 2).

By E-Mail:

Send support requests to nodehelpdesk@csc.com

Version 1.1 DNCs

- **Java-based (Integrated Client and Server DNC)**
  - **Apache Axis 1.1** – DNC can be used with any Java-Based middleware, (e.g., WebLogic, WebSphere, XAware, Oracle 9i)

- **Microsoft .NET DNCs**
  - DNC for server side using Microsoft .NET C#. This requires .NET framework 1.X and WSE 1sp1.
  - DNC for server side using Microsoft .NET VB . This requires .NET Framework 1.X and WSE 1sp1. DNC (executable files) for client side (to generate requests) for Microsoft .NET.
  - Sample client for .NET This is a sample client that uses the included requestor library (CDX_DOTNET_REQUESTOR.DLL). This library is all that is needed to communicate with a Node from any .NET language (e.g., VB, C#, J#). Only requires the .NET Framework 1.X and WSE 1sp1.
  - Also available is a C# client library (.zip file). This allows you to change the requestor library above. If you don't want to change the API, you should download the .NET Sample Client. Requires the .NET Framework 1.X and 1sp1.

- **All Tools available on the Exchange Network Website "Tool Box" Section**

Test Tools

https://test.epacdxnode.net/test/

- This application provides the ability to test any Node in the Exchange Network, by triggering Network WSDL-compliant requests on that Node.
- If a Node passes a test with this tool, it is very likely, the Node will be interoperable with other Network WSDL-compliant Nodes.
- This tool, which is intended to verify general compliance with the Functional Specification, focuses on interoperability among Nodes. Testers can choose to perform either:
  - interactive tests
  - automatic tests.

Guidance and Technical Documents

- Network Node Functional Specification v1.1
- Network Exchange Protocol v1.1
- Node Implementation Guide v1.0
- Flow Configuration Document Template v1.0*
- Node, Flow, and Client Definitions and Implementation Statuses

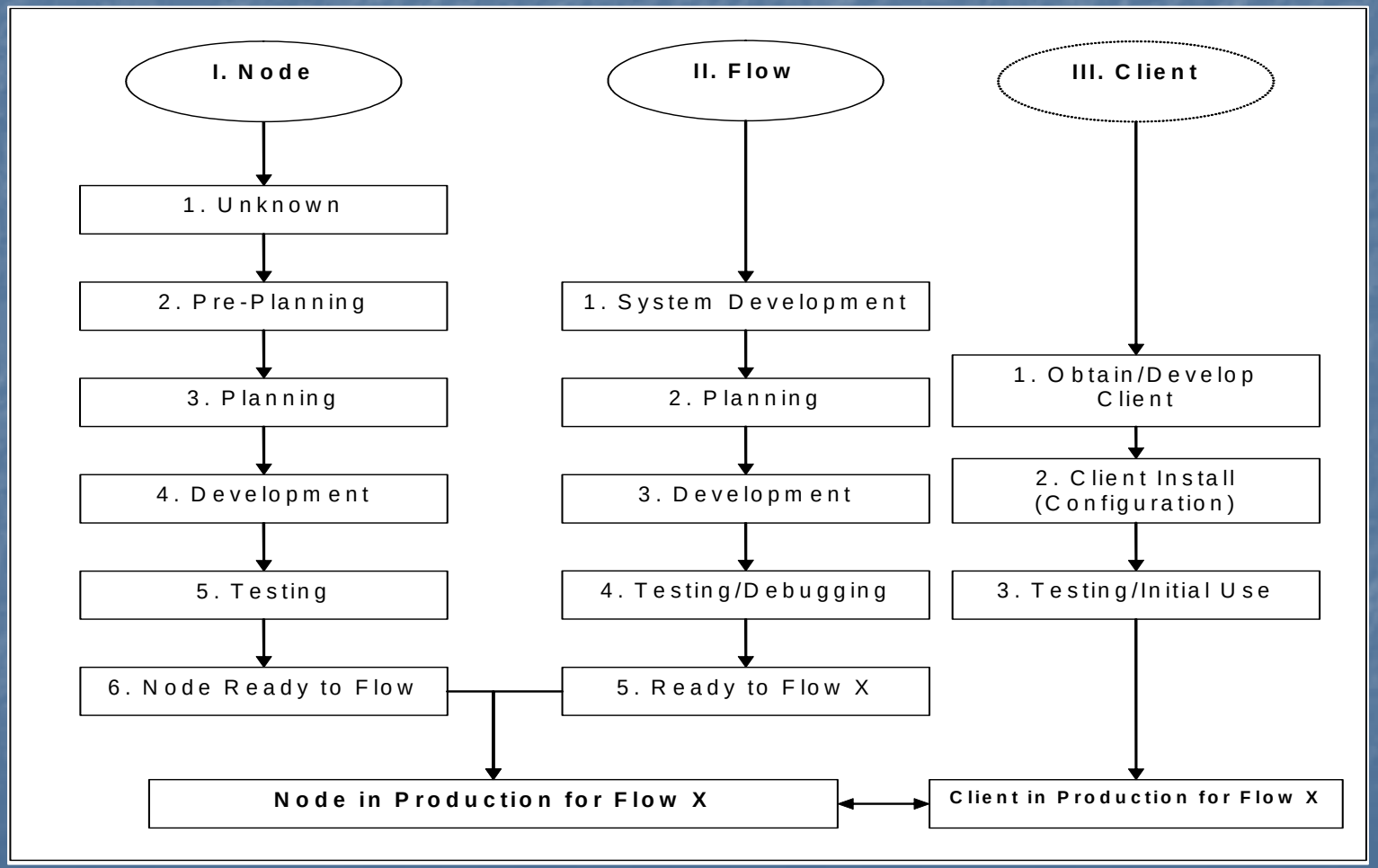
* Available February 2004

- Administrator's Guide to Network Security*
- Network Security Policy Document v1.0*
- Network Security Specifications
- Network Security Guidelines
- Network Security White Paper
- Core Reference Model
- XML Schema Design Rules

Node Mentoring Group

- Node Mentoring Group National Meeting – “Sharing What We Node”
  - New Orleans, February 9th-10th, 2004.
  - Workshop sessions will include topics such as the " Practical Do's and Don’ts of Setting Up Nodes" and presentations by leading web services vendors and Node pilot project vendors.
  - The workshop venue is the Royal St. Charles Hotel in New Orleans (1-866-658-4737). Those interested in attending the workshop should make hotel reservations by January 15, 2004.
  - For more information about the Workshop, contact David Ellis via email at david.h.ellis@maine.gov.

Flow Deployment



Flow Deployment: Requirements and Resources Available

Deployment	Requirements	Resources Available
1. System development	➢ System development documented	➢ State experiences ➢ Flow pioneers
2. Planning This includes identifying datasets to flow and planning for resources to map Schema to databases.	➢ Flow deployment scheduled (internal)	➢ State experiences
3. Development Linking from Node to source system, mapping to target Schema, and establishing business rules and workflow.	➢ Draft Partner FCD for Flow X completed ➢ Backend databases to Schema mapped	➢ Flow Configuration Document Template or Flow Configuration Document for Flow X
4. Testing / Debugging Partners are performing Node-to-Node and end-to-end testing of the flow.	➢ Flow Node-to-Node test suite successful processed ➢ Flow end-to-end test suite (i.e., from source system, through Nodes/client, to destination system, with exchange acknowledgement) successfully processed ➢ Query/Solicit (Data Requests) successfully tested	➢ Revised deployment schedule ➢ Flow Configuration Document (FCD) for Flow X ➢ Test Tool
5. Ready to Flow X The Flow has passed all testing and is ready to exchange data over the Network.	➢ Final Partner FCD for Flow X completed ➢ Final deployment scheduled	➢ N/A

Status of Current Schema and Flow Development

XML Schema	Status	Type	EPA Can Receive into Systems	Flow Through CDX Web Interface
Beach (3 flows)	Complete	State/EPA	Yes	
FRS	Complete	State/EPA Voluntary	Yes	√
NEI	Complete	State/EPA Regulatory	Yes	
eDMR	Complete	Industry to State		√
PCS/IDEF	Complete	State/EPA Regulatory	Yes - not simple	
Drinking Water	Complete	Industry to State	N/A	
SDWIS	Close	State(SDWIS) to EPA regulatory	No	
RCRAInfo - EPA 3 modules	In Progress	State/EPA Regulatory	No	
RCRAInfo - Pilot Project All modules	In Progress	State/EPA Regulatory	No	
Manifest	In Progress	State to State	N/A	
Surface Water (piece of STORET)	In Progress	State to State	N/A	
Institutional Controls	In Progress	State/EPA Voluntary	No	
AQS	In Progress	State/EPA Regulatory	No	
Laboratory Drinking Water	Coordinating	Labs to State	N/A	
STORET	Not Started	State/EPA Regulatory	No	
TRI	Not Started	EPA to State	N/A	
AFS	Not Started	State/EPA Regulatory	No	

The Flow Configuration Document

The Flow Configuration Document (FCD) Template identifies the universe of information Network Partners should consider when documenting and implementing a *Flow* or a *Common Data Service*.

- A Flow Configuration Document may include, by reference, information from many other documents (Schema, system code lists, or procedures).

Network Security

Network Security Risks

The following is a list of typical threats to information security in distributed Web services network.

- Unauthorized Access to Web Services
- Unauthorized Information Flow
- Vandalism and Sabotage
- Theft and Fraud
- Violation of Data Integrity

Security Definitions

- **Secure Socket Layer (SSL):** specifies a mechanism for providing data security layered between application protocols.
- **Hyper Text Transport Protocol Secure (HTTPS):** This is HTTP using SSL. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80.
- **Public Key Infrastructure (PKI):** uses a pair of asymmetric digital keys to encrypt transmitted data. The PKI model also involves certificate authorities issuing certificates with public asymmetric keys and authorities that assert properties other than key ownership (for example, attribute authorities).

Authentication Definition

- Authentication is the process of verifying that a subject, either a user or a machine, is who they claim to be. The authentication process requires that the subject present evidence, or a credential. The credential is then checked or verified against an authority.
- Types of Authentication:
  - User Authentication
  - Machine Authentication
  - Message Authentication

Authorization Definition

- Authorization is a process that establishes entitlement of a user. The user or principal, although authenticated, may not be allowed to access certain network services based on a security policy. Given the authenticated user identity (the subject) and the security policy of a network resource (the object), a Network Node can determine whether or not to grant access.
- Authorization determines whether the service provider has granted access to the Web service to the requestor. It answers the question:

  Is operation X by principal Y on resource Z permitted?

Network Security Requirements

There is no such thing as perfect security. However, a Network Node is considered secure or strong if it meets the following general requirements:

- **Authentication**
- **Authorization**
- **Confidentiality**
- **Message Integrity**
- **Non-repudiation (optional)**

Centralized Security Approach

- Given the number of Nodes on the Network and the diversity of IT environments, it is unrealistic to require all Nodes to develop and deploy similarly strong security components.
- It is necessary to develop components or Web services that can be shared or reused by all Nodes. "Centralization" is fundamental to reducing development and administrative costs, and complexity.
- Although centralized services are resources to Nodes, their usage is not mandatory. Nodes can still leverage existing security infrastructure and perform additional verification and validations if necessary.

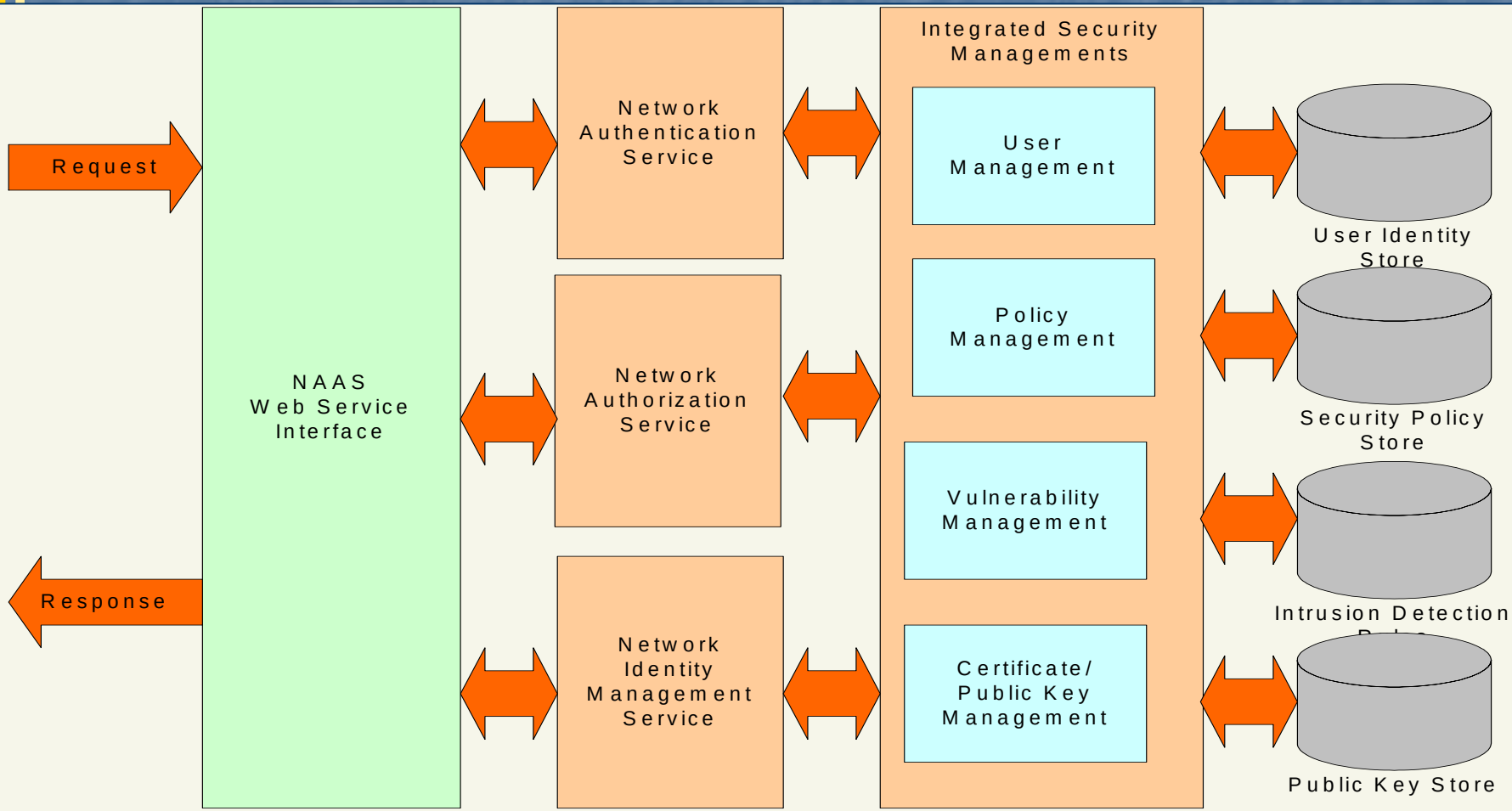
Network Security Infrastructure aka NAAS

- **NAAS Web Service Interface:** SOAP service that exposes user authentication and authorization functions to all state Nodes. It is the entry point for all service requests.
- **Network Authentication Service**: This is a subsystem for verifying subject (user or machine) identity.
- **Network Authorization Service**: This component is for entitlement management. Authorization is typically role-based or policy-based. It must be flexible so that a variety of factors can be part of the decision to grant or deny access to specific resources.
- **User Identity Management:** This component is responsible for registering users, removing users, and modifying user profiles.
- **Policy Management:** The component allows administrators to create or modify rules or policies for resource access.
- **Vulnerability Management:** This component tracks instances of security breaches and generates reports that contain specific information about vulnerability and actions taken. A good vulnerability management system helps to prevent security problems from recurring.
- **Network Certificate Authority:** This component issues and manage certificates used for SSL, encryption and signature.
- **Public Key Management :** This component allows users to locate and validate public keys.

Why NAAS?

- Simplify Implementation
- Enhanced Security
- Cost Effective
- Highly Extensible
- Support Single Sign-On (SSO)
- Security Monitoring

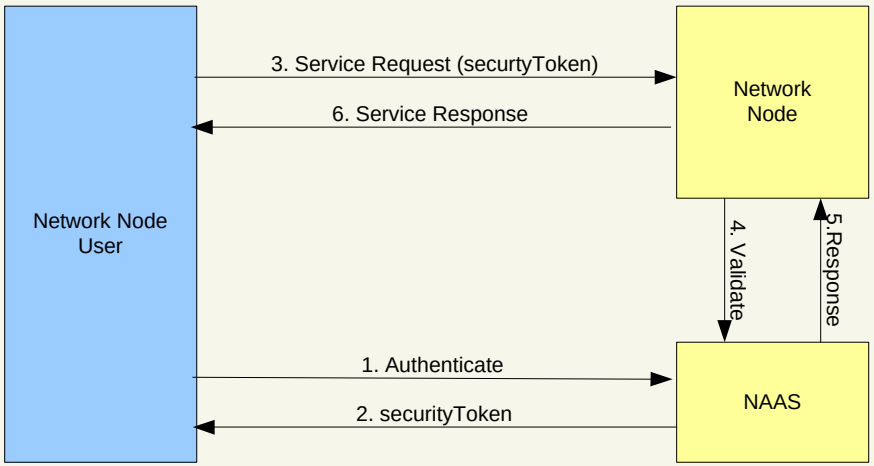
Network Security Infrastructure



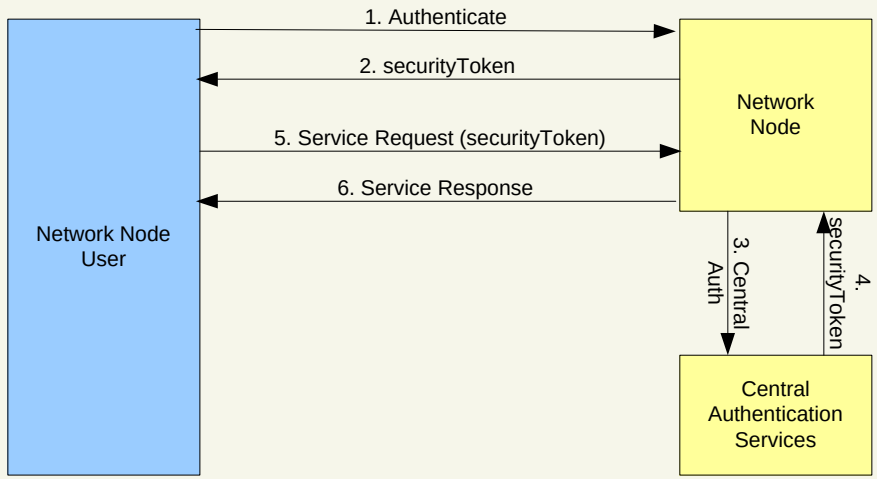
Environmental Information eXchange Network

Authentication on the Network

Direct Authentication: the client sends Authenticate messages to the NAAS and obtains a securityToken.



Delegated Authentication: the client sends an Authenticate message to a Node. The Node then delegates the authentication request to the NAAS for processing using the CentralAuth method.

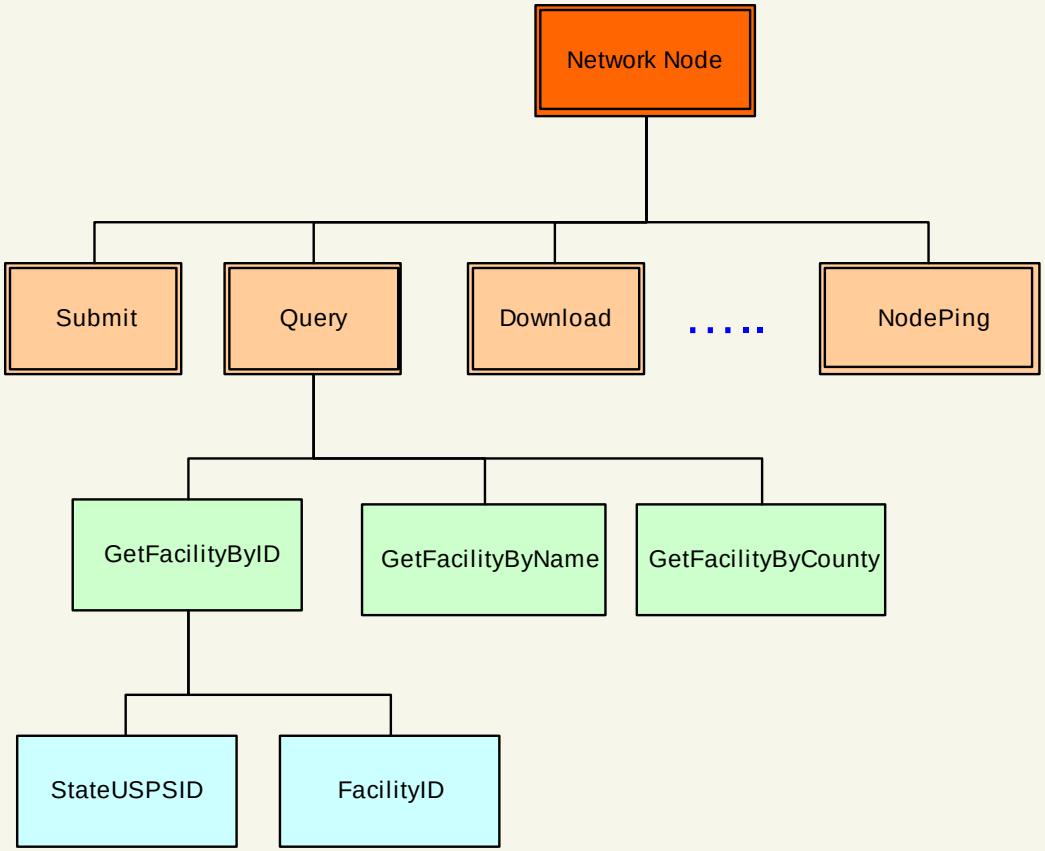


Authorization on the Network

The Network Authorization service provides multi-level access controls. The following are the levels of authorization:

- **Node:** Node is the top level of Access Control. When a subject does not have access to a Network Node, requests to all Web methods will be denied.
- **Method:** Method is a child level of Node. When a subject does not have access to a Web method, the requested operation will be rejected. For example, if a user is not allowed to use the Query method, all service requests using Query will be denied.
- **Service Request:** Service Request is a child level of Method. It applies to the Query, Solicit, and Execute methods. In the Network Node Functional Specification, Service Requests (stored database procedures) are one of the parameters in the Query method. Service Request level control allows administrators to determine whether or not a person can perform a database query.
- **Parameter:** Parameter is a child level of Service Request. A database query (Service Request) may require parameters that determine the scope of the query. Parameter level access control can effectively limit what a user can see in the result set.

Network Authorization Structure



Node

Method

Request

Parameter

Authorization Defaults

Based on the type of the user, the following default policies apply:

- Administrators: When an administrator account is created, the administrator has ***all access rights*** to the Node they manage, including managing user accounts, create authorization policies, and invoking methods at the Node.
- Operators: When an operator account is created, the operator, by default, can conduct ***dataflow operations*** at the Node they belong to, which means that the operator has access rights to the Web methods provided by the Node.
- User: When a regular user account is created, the user has ***no access rights*** to the Node by default. Administrators need to grant rights by explicitly creating authorization policies.

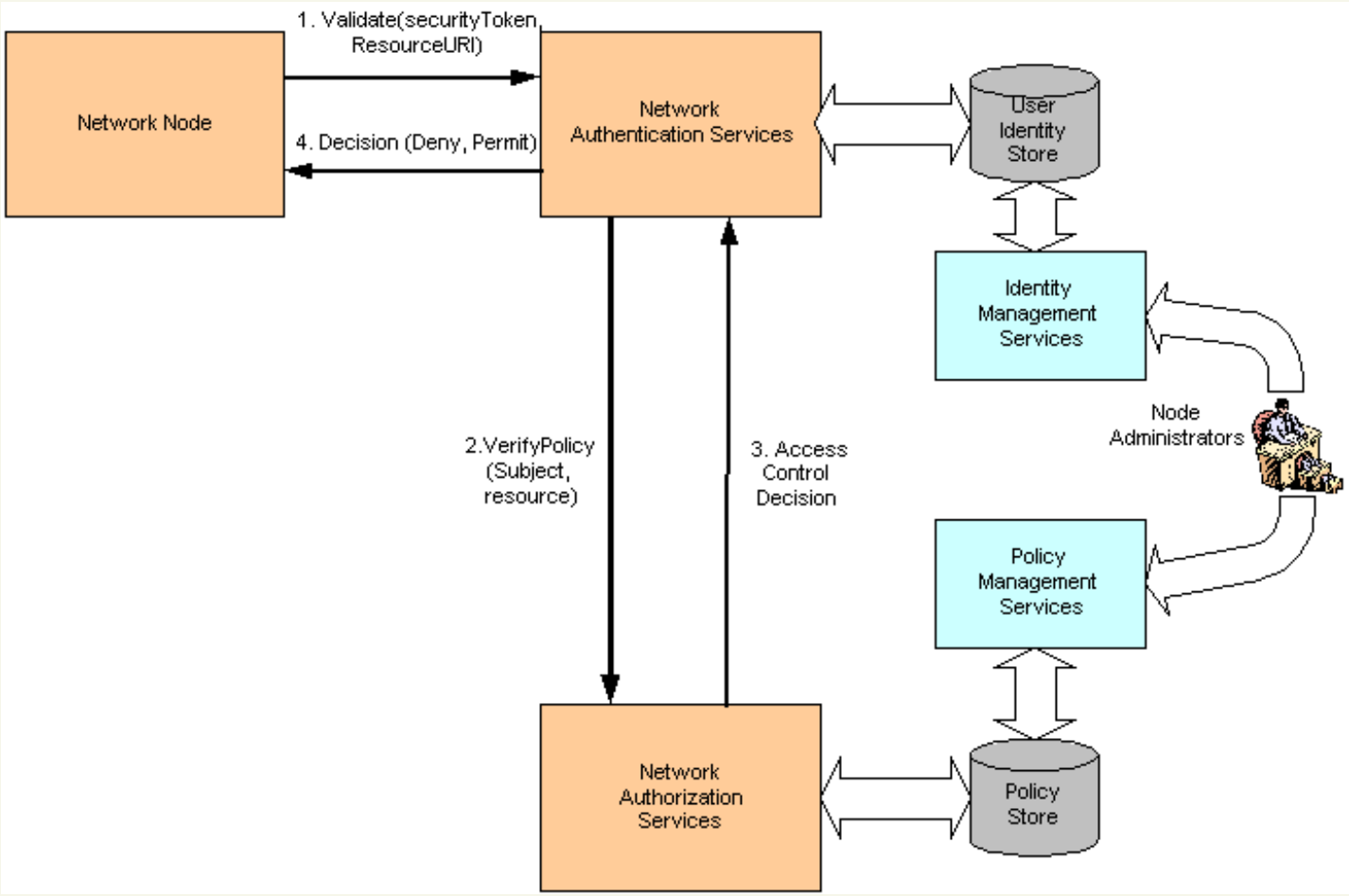
Trust Certificates

- Trust Certificates are a way to prove the validity of an entity's public key and may well be the future mechanism to provide single login capabilities in today's corporate networks.
- The NAAS will act as a Network Certificate Authority (CA) i.e. the trusted third party that vouches for the validity of the certificate. It is up to the CA to enroll certificates, distribute certificates, and finally to remove (revoke) certificates when the information they contain becomes invalid.

Exchange Network CA Services

- Issue SSL Certificate for Network Node.
- Issue certificate to network users for network authentication.
- Validate user certificates.
- Verify Digital Signature.
- Establish trust relationships among network nodes.

Putting it all together



Establishing NAAS Accounts

- Three types of NAAS Accounts
  - Test Accounts
  - Node Administrator Accounts
  - User Accounts
- Test and Node Administrator accounts established by calling the Network Help Desk
- User accounts established by the appropriate Node Administrator

NAAS Test Accounts

- Test accounts can be established to assist during Node implementation and testing.
- Test accounts expire after X days
- All interactions with the NAAS must use SSL
- Current ubiquitous test account expires January 20th, 2004.

Node Administrators

- All Nodes must establish a security contact and obtain NAAS Node administrator's account.
- Account established by calling the Network Help Desk.

Being a Node Administrator

A Node Administrator has the right to:

- Add Users
- Delete Users
- Get User List
- Change Passwords

Node Administrator's Policy Management Privileges:

- Set Policy
- Delete Policy
- Verify Policy
- Get Policy List
- Get Auth Events

Managing your Account: NAAS GUI

- The Network Authorization Service offers a set of XML Web Services for administrators to manage access control rules and policies. The operations can be performed using either a Web browser or other applications capable of processing SOAP messages. All messages in the authorization service are SOAP/RPC encoded, and they must be sent over SSL.

Security Resources

- Network Help Desk
- Administrator's Guide to Network Security* - February 2004
- Network Security Policy Document* - January/Early February 2004
- Network Security Specifications* - Complete
- Network Security Guidelines - Complete
  available at http://www.exchangenetwork.net.
- Network Security White Paper - Complete
  available at http://www.exchangenetwork.net.

** Document will only be made available to Node Administrators.*

Questions?

NAAS Demonstration