



Common Secure Interoperability Version 2 CSI v2

A User's View
by
Don Flinn

The Specification Team



Compaq

IONA/OOC

Concept Five

Oracle

Gemstone

Persistence

Hewlett Packard

Promia

IBM

SUN

Inprise

Syracuse/Adiron

CSI v2: What, Why, How



- What
 - Secure Interoperable Wire Protocol
 - Support authentication, delegation & privileges
- Why
 - Define a CSI Architecture
 - Support SSL & Interoperate with EJB
- How
 - Tightly Define
 - Wire Protocol, Messages, IDL
 - Support Interoperability using SSL and optionally SECIOP

CSIv2 Status



- CSI v2 has been passed by vote of the OMG Architecture Board
- CSI v2 has been accepted/referenced by EJB version 2.0
- CSI v2 is undergoing the FTF process of the OMG
 - Editorial
 - Correct Errors in Found in Implementation

What CSIv2 Can Do For You



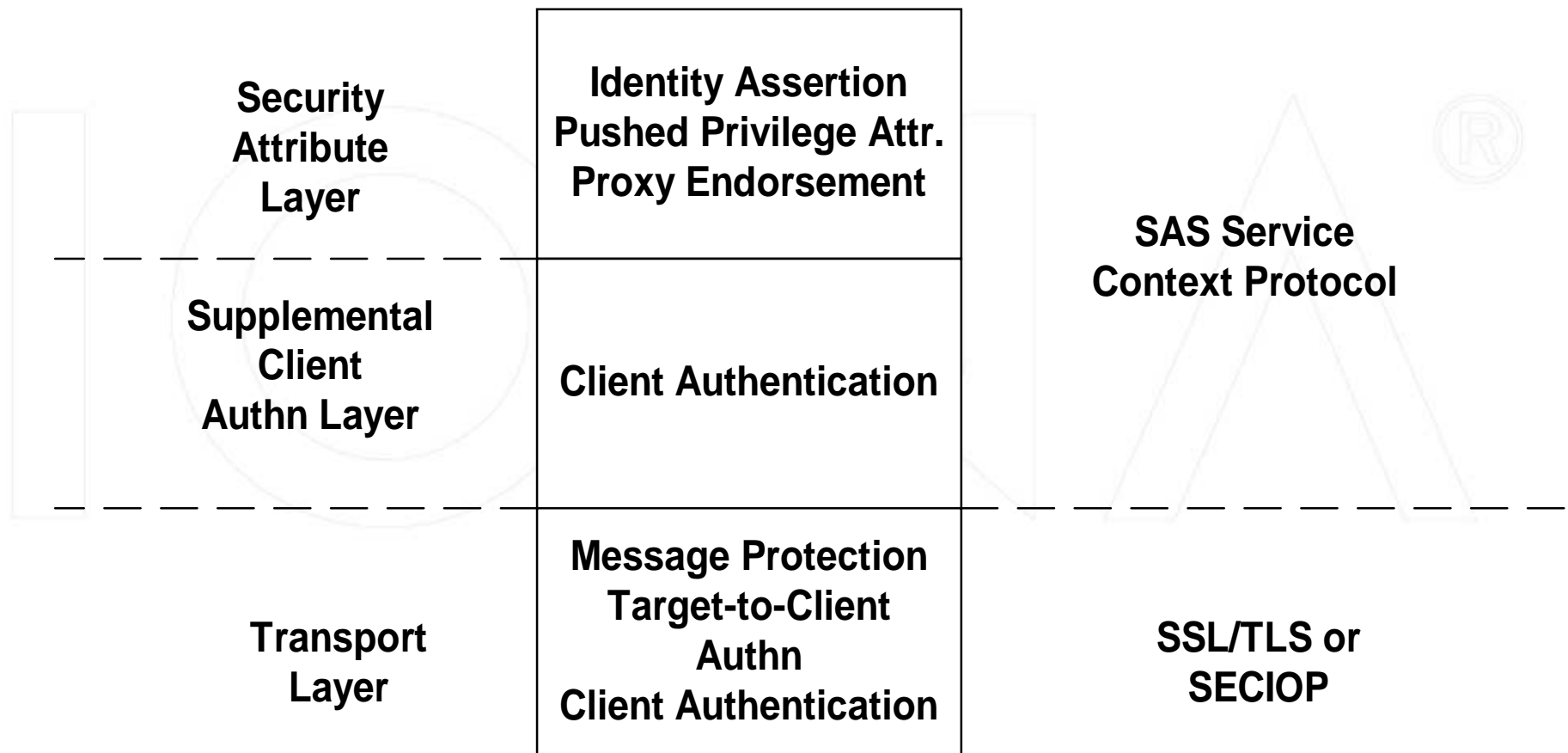
- Secure Interoperability
 - CORBA to CORBA
 - EJB / CORBA
- Extended Attributes for Authorization
 - Standard Credential (PAC)
- Delegation
 - Both Simplified and Extended
- Federation
 - Lay the Groundwork

CSlv2 Flexibility



- Different Transport Layer Protocols
 - SSL Required
 - X.509 Certificates
 - Supported by GSSUP username/password
 - SECIOP
 - Kerberos, SPKM, CSI-ECMA
- Stateful or Stateless
- Degrees of Authorization
 - UserName to PACs
- Multiple Forms of Delegation

Secure Attribute Service (SAS) Protocol



SAS Messages



- EstablishContext
 - Sent by Client to Establish Context
- CompleteEstablishContext
 - Sent by Target to Acknowledge
- MessageInContext
 - Sent by Client in Stateful Session
- ContextError
 - Sent by Target if Error in Establish Context

Simple Example



- Client Securely Interoperate w/ Target
 - Pass Security Data
 - Use the Service Context in Request/Reply Header & Optionally Transport Layer
 - Type of Data
 - Authentication
 - Transport Layer (SSL Certificate)
 - Authentication Layer (GSSUP)
 - Authorization
 - Name
 - Privilege Attribute Certificate (PAC)

UserName/Password GSSUP



```
// GSSUP::InitialContextToken
struct InitialContextToken {
    Security::UTF8String username;
    Security::UTF8String password;
    CSI::GSS_NT_ExportedName target_name;
};
```

target_name contains the name of the authentication domain in which the client is authenticating.

Privilege Attribute Certificate (PAC)



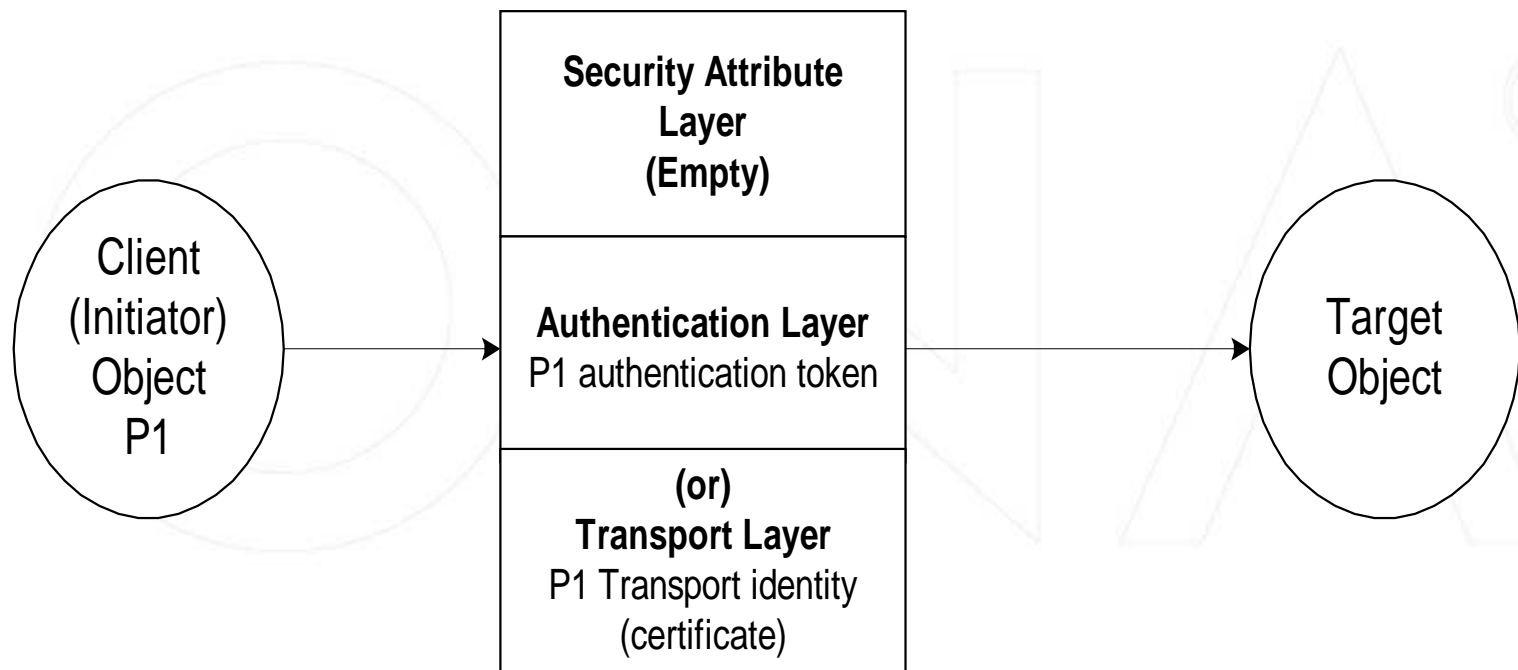
- **AttributeCertificate ::= SEQUENCE {**
- **acinfo AttributeCertificateInfo,**
- **signatureAlgorithm AlgorithmIdentifier,**
- **signatureValue BIT STRING**
- **}**

- **AttributeCertificateInfo ::= SEQUENCE {**
- **version AttCertVersion DEFAULT v1,**
- **holder Holder,**
- **issuer AttCertIssuer,**
- **signature AlgorithmIdentifier,**
- **serialNumber CertificateSerialNumber,**
- **attrCertValidityPeriod AttCertValidityPeriod,**
- **attributes SEQUENCE OF Attribute,**
- **issuerUniqueID UniqueIdentifier OPTIONAL,**
- **extensions Extensions OPTIONAL**
- **}**

Simple Interoperability



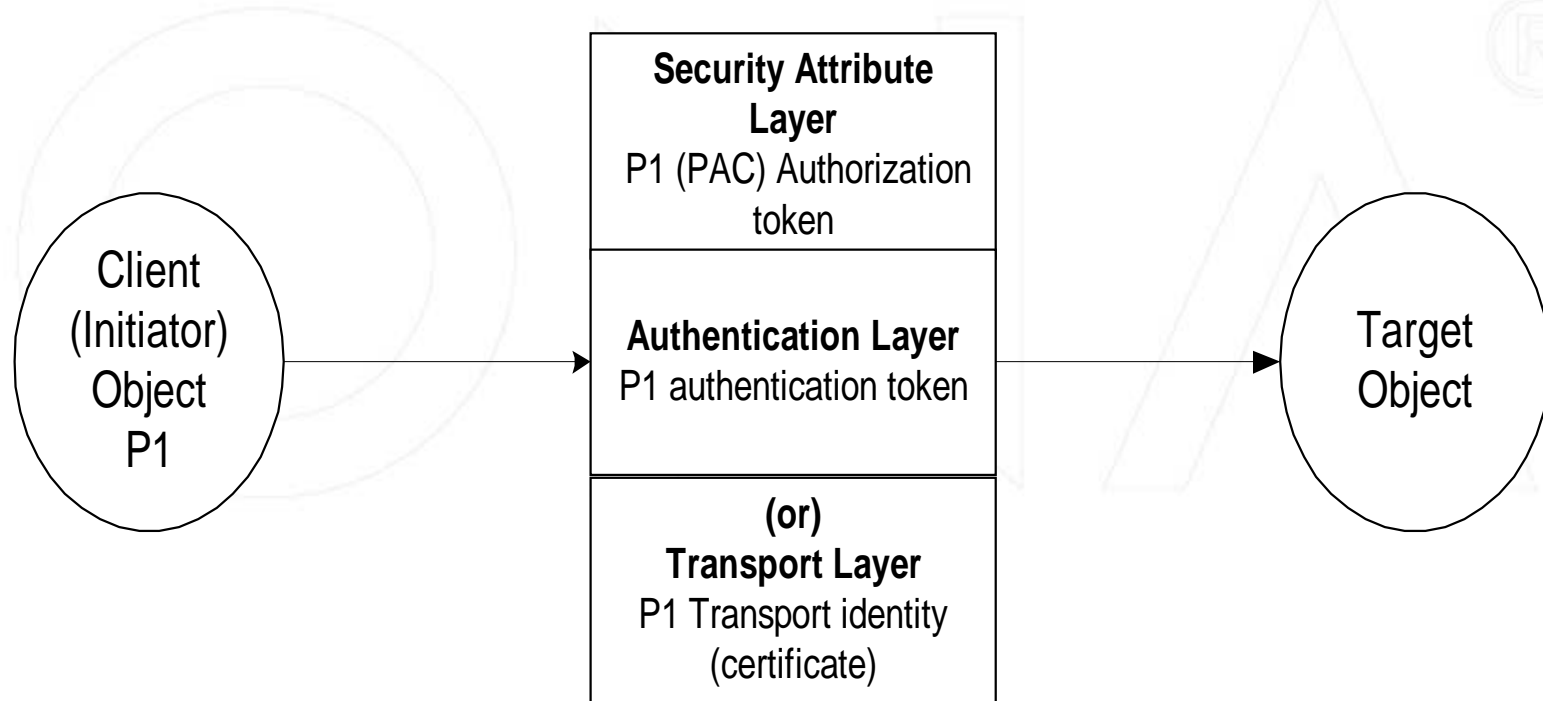
CSlv2 Credentials Tokens



Push Privilege Attributes



CSlv2 Credentials Tokens



Delegation



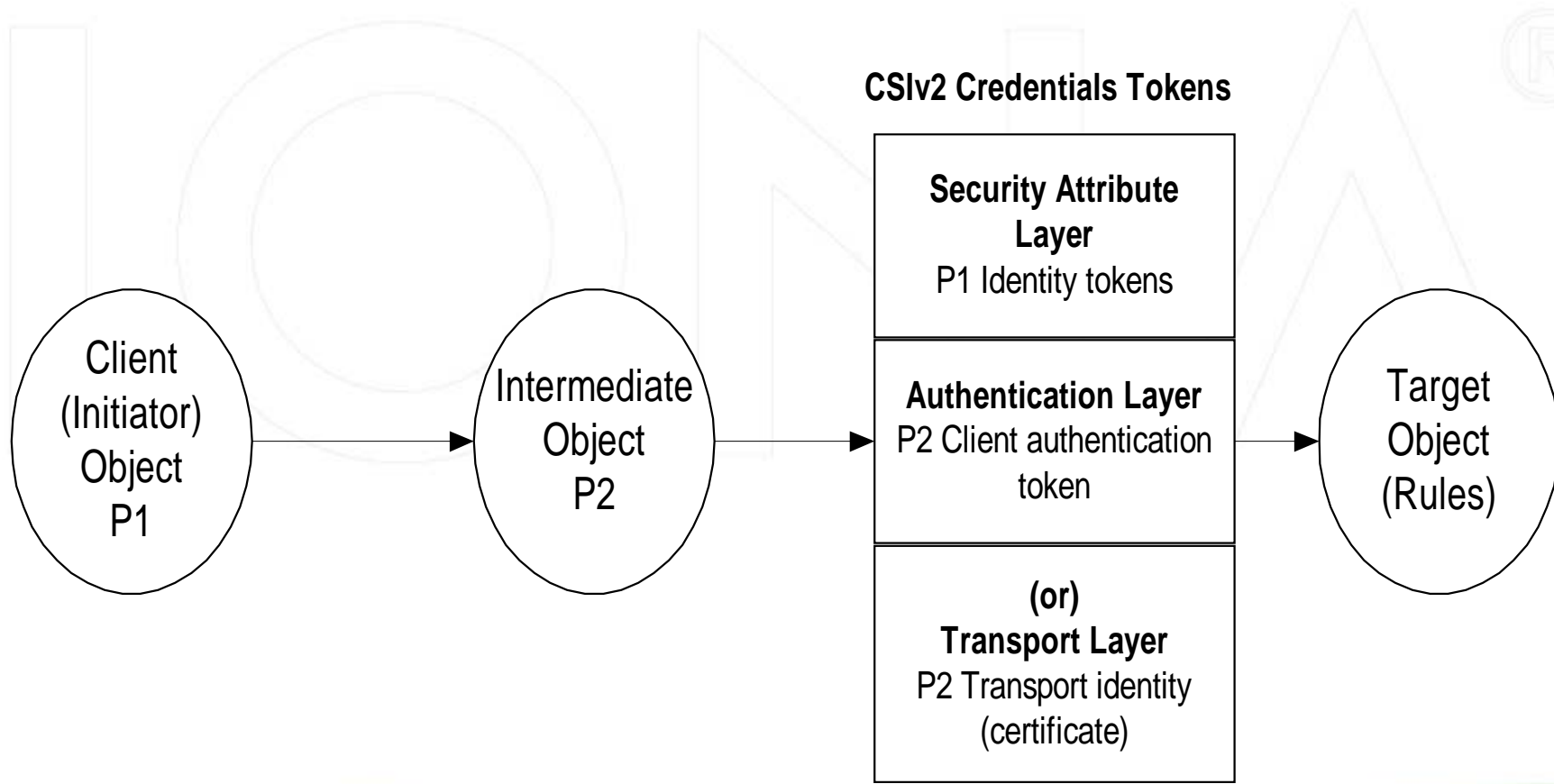
- Delegation Data
 - Identity Token or PAC
- Types of Delegation
 - Authorization token-based delegation
 - Forward trust evaluation
 - Identity assertion-based delegation
 - Backward trust evaluation
 - Presumed trust

Identity Token



- Carries the “Spoken For” or Asserted Identity
- Identity Token Types
 - Absent
 - Anonymous
 - Principal Name
 - Distinguished Name
 - X.509 Certificate Name

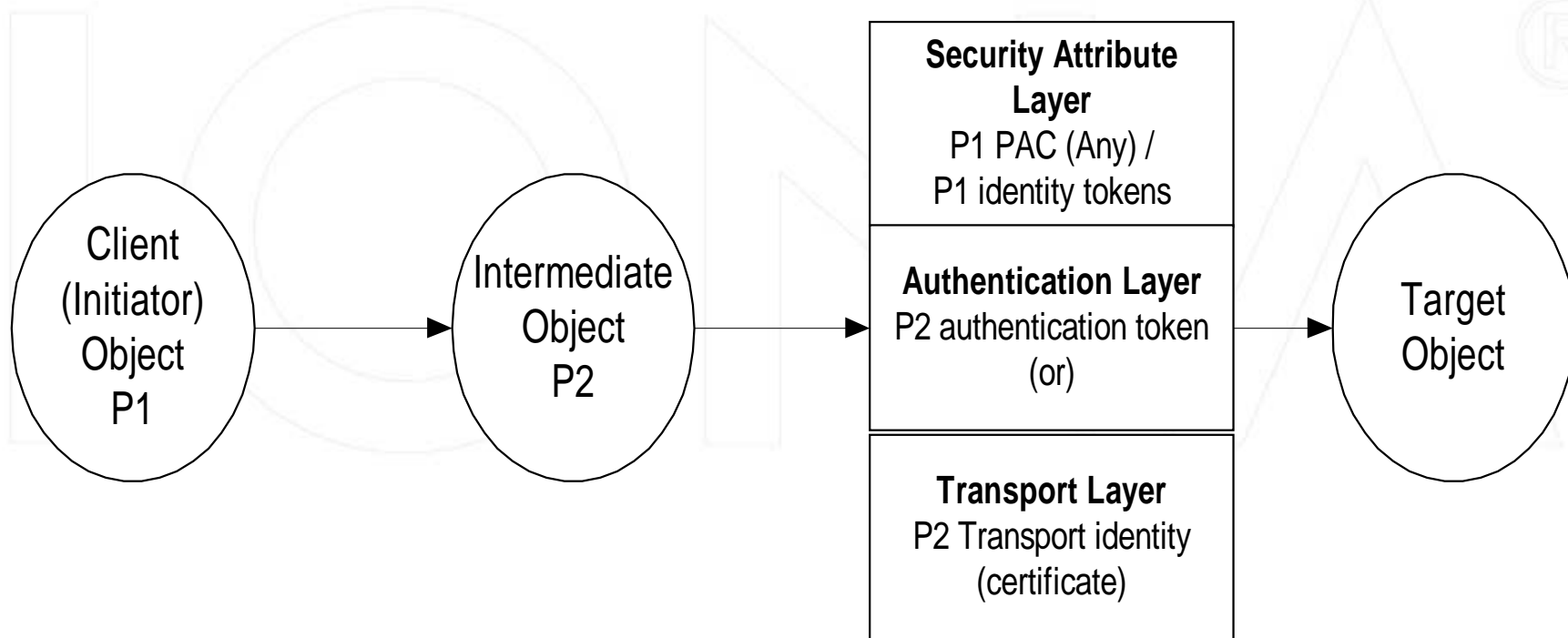
Delegation - Backward Trust



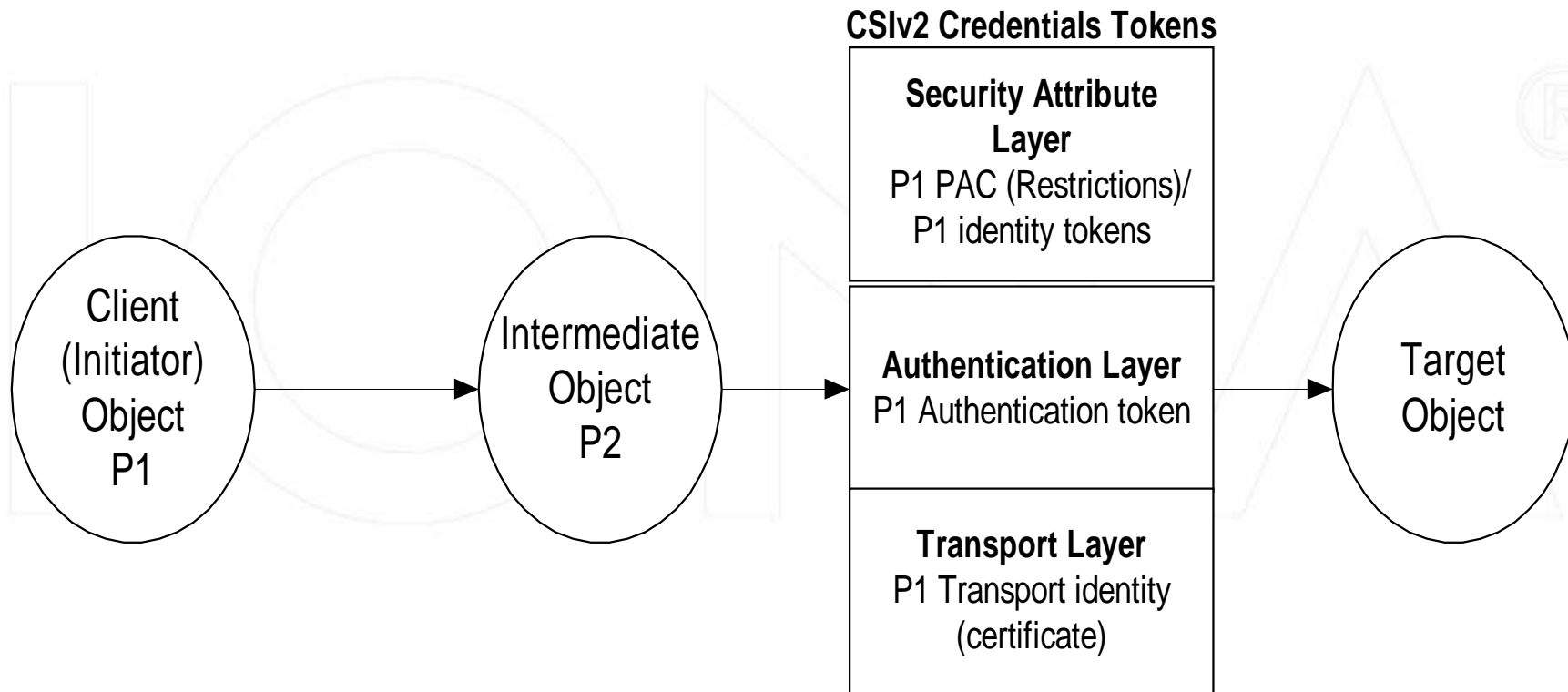
Delegation - Forward Trust



CSlv2 Credentials Tokens



Delegation - Restricted



Delegation con't



Examples of CSIV2 Credentials Passed from Intermediate to Target

Security Layers	1 No delegation	2 No delegation, push privilege attributes	3 Identity assertion- based delegation, backward trust evaluation	4 Authorization token-based delegation, forward trust evaluation	5 Authorization token based delegation (restricted), forward trust evaluation
Security Attribute Layer Authorization/ identity tokens	--	P2 PAC	P1 identity token	P1 PAC, "Any" proxy attribute; P1 identity token	P1 PAC, P2 identity proxy attribute; P1 identity token
Authentication Identity Client authentication token or transport identity	P2 identity	P2 identity	P2 identity	P2 identity	P2 identity
Target Validation Checks	--	P2 PAC belongs to P2 identity	P2 permitted to speak for P1 identity based on rules of the target; presumed trust if target has no rules	P1 PAC belongs to P1 identity; "Any" proxy attribute permits any intermediate to use P1 PAC (unrestricted delegation)	P1 PAC belongs to P1 identity; P2 identity proxy attribute permits P2 to use P1 PAC (restricted delegation)

Conformance



- Level 0
 - SSL/TLS & GSSUP
 - Stateless
 - SAS - Identity Assertion
- Level 1
 - Authorization Token (Push)
- Level 2
 - PAC with Delegation
- Stateful Conformance