



WinFX



Windows Communication Foundation

Parte 3/3

Paolo Pialorsi
paolo@devleap.it

DevLeap

<http://www.devleap.com/>

The DevLeap logo, featuring the word "devleap" in a bold, sans-serif font. The "v" is stylized with a blue checkmark and a small figure jumping over it. The logo is set against a white background with a blue border.

Brevissima presentazione

- Sapete cosa facciamo
 - Consulenze, Conferenze, Corsi
 - Sviluppo ad hoc
 - Libri, articoli, multimedia
- Competenze
 - .NET Framework 2.0
 - SQL 2005 sia OLTP che BI
 - Mobile con VS 2005 e .NET CF 2.0
 - Software Architectures
 - WinFx



Argomenti di oggi

- Teoria della sicurezza SOAP (Quick)
 - WS-Security
 - WS-SecureConversation
 - WS-SecurityPolicy
 - WS-Federation
 - WS-*
- Autenticazione
 - Windows
 - Username/Password
 - X.509 Certificates
 - Kerberos
 - InfoCard
- Autorizzazione
 - Host Gate
 - Operation Contract Gate
 - Application Gate
- Integrità e Riservatezza
- Q&A

WCF ad oggi è in Beta

Quello che vediamo potrebbe cambiare da qui al rilascio.

Nelle slide e demo ci riferiamo a:

Beta2 CTP Feb 2006 e/o Beta2 CTP Maggio 2006



WinFX

Sicurezza del Protocollo



- Tutti devono “conoscere” il protocollo
 - Gli intermediari devono “interpretare” gli header del messaggio
- Cripta/firma l'intero messaggio
- Legato al protocollo

XML Signature

- È una raccomandazione del W3C del 12/2/2002
 - (<http://www.w3.org/TR/xmlsig-core/>)
- Descrive una grammatica XML (schema) da applicare ad un messaggio XML per firmarlo o per firmare alcune delle sue parti
- Prevede la normalizzazione del messaggio prima della firma
 - `<titolo/>` e `<titolo></titolo>` hanno lo stesso significato semantico
 - Ma fornirebbero digest diversi!

WS-Trust

- Esistono diversi modelli di trusting
- Tutti si basano sul concetto che:
 - ci deve essere qualcuno che garantisce per un altro
- Spesso sarà il client a richiedere che qualcuno “lo presenti” al server
- Il client dovrà a sua volta rendersi “credibile” (tramite un token) al Trust server

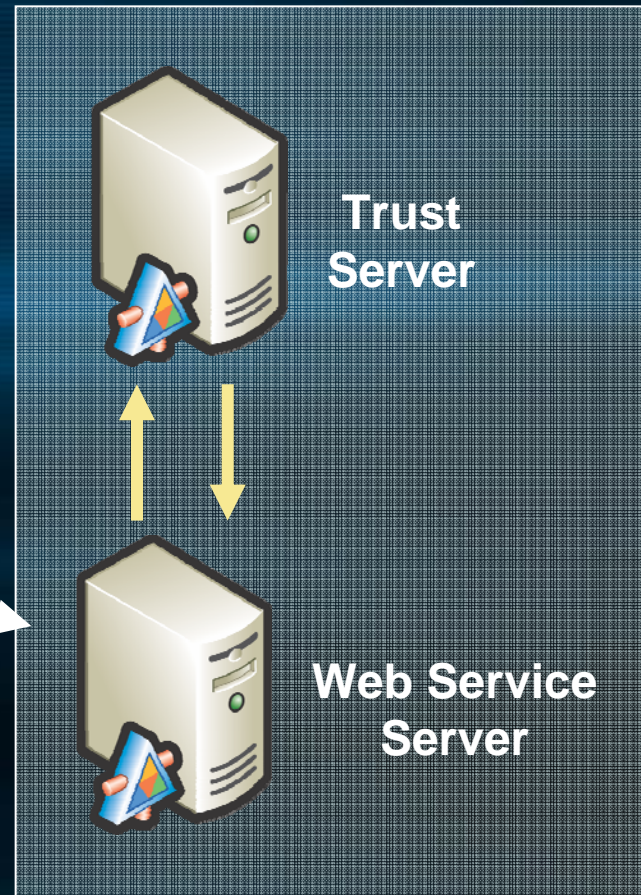
WS-Trust (1° modello)

- Consente di utilizzare una trusting authority centralizzata alla quale si rivolge il client prima di chiamare il server



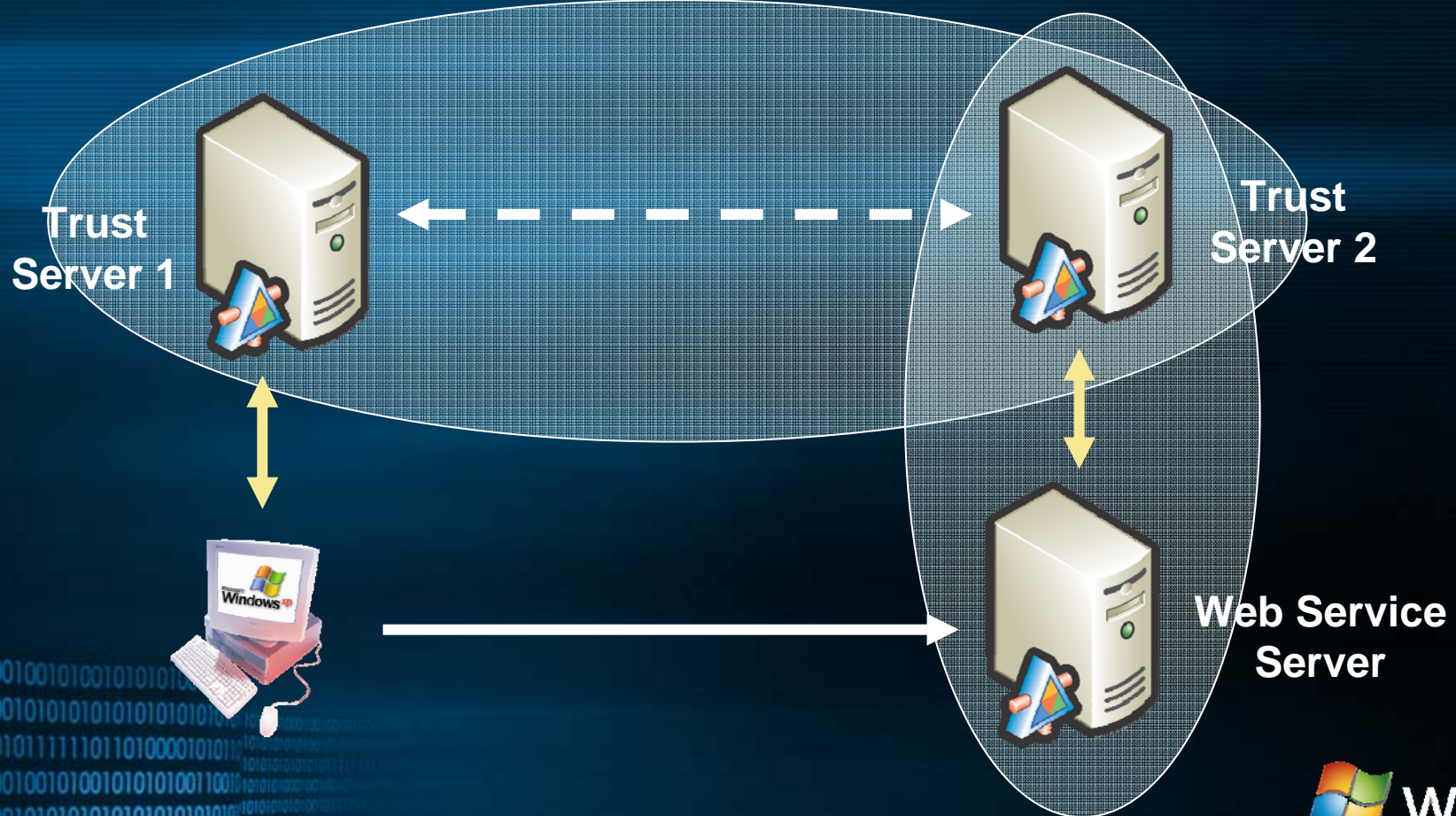
WS-Trust (2° modello)

- In questo caso è il server che si preoccupa di ottenere il token per il client



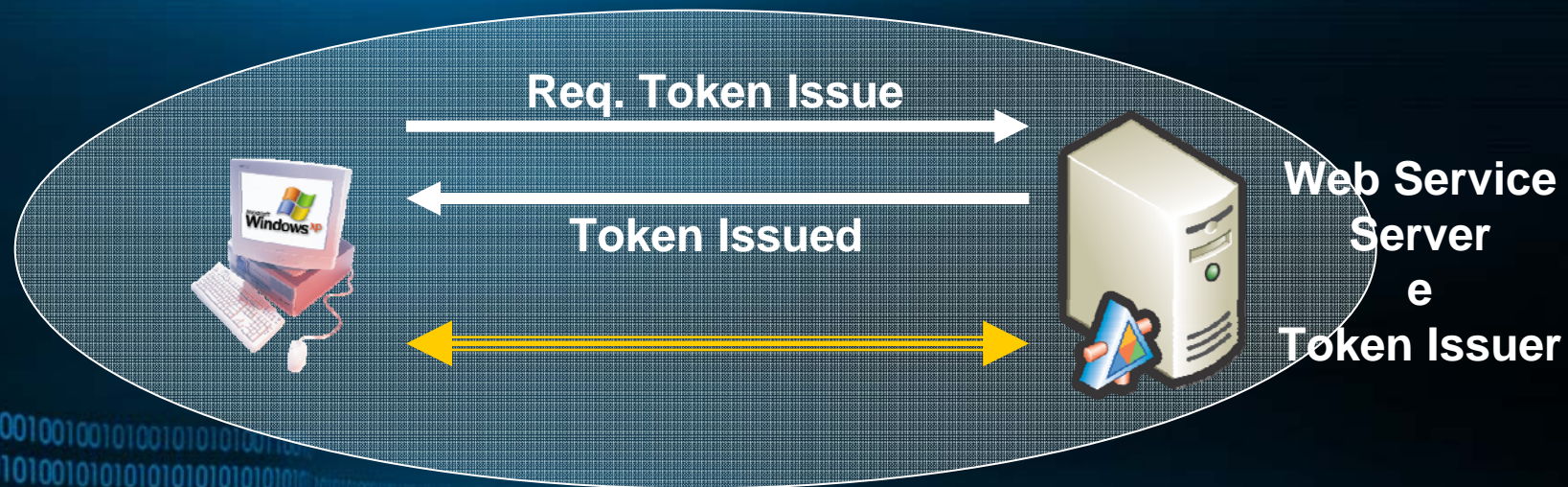
WS-Trust (3° modello)

- Consente di utilizzare una trusting authority centralizzata



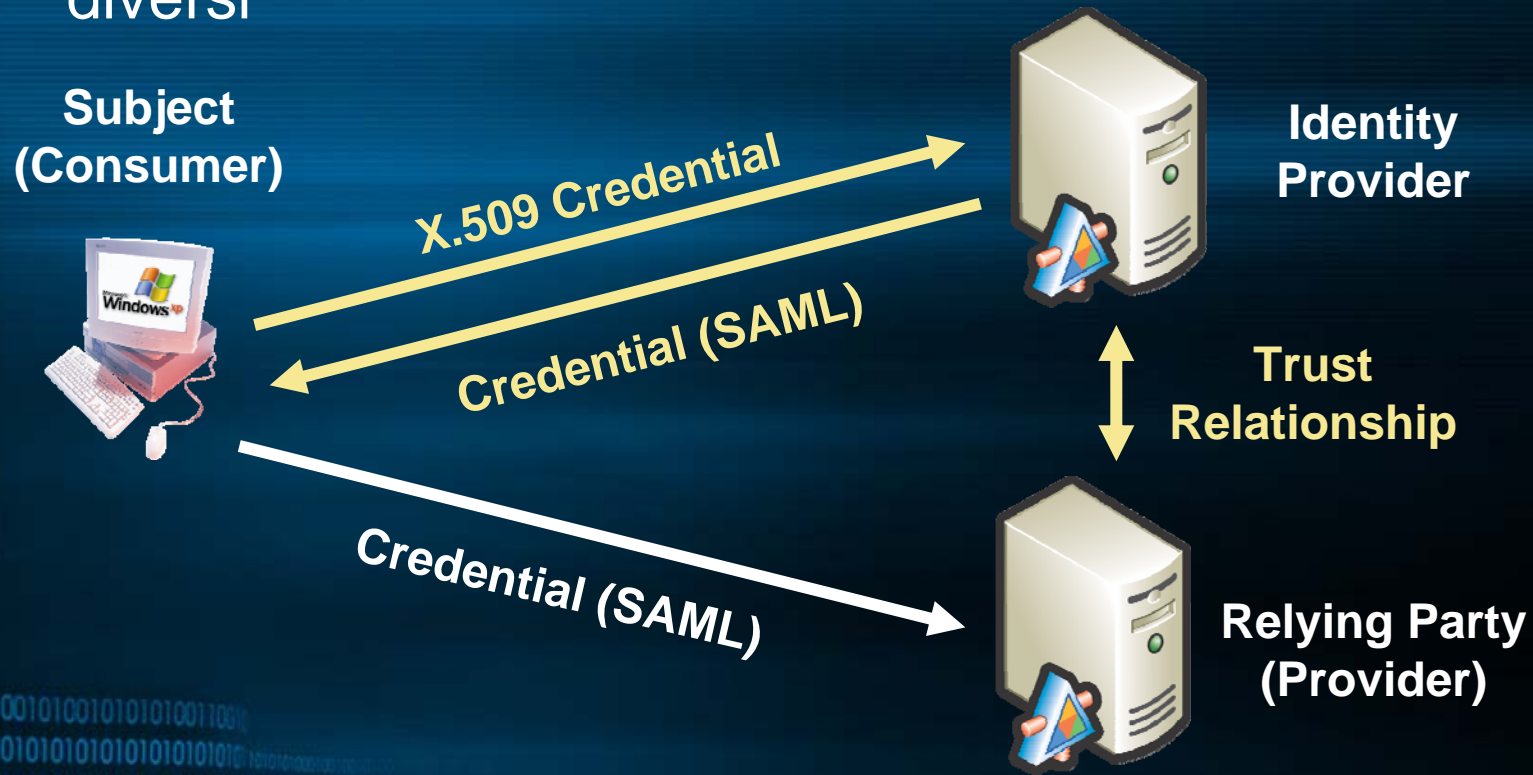
WS-SecureConversation

- Quando il server e il client si scambiano un token “di sessione” (SCT)
- Finalizzato alla singola sessione di conversazione



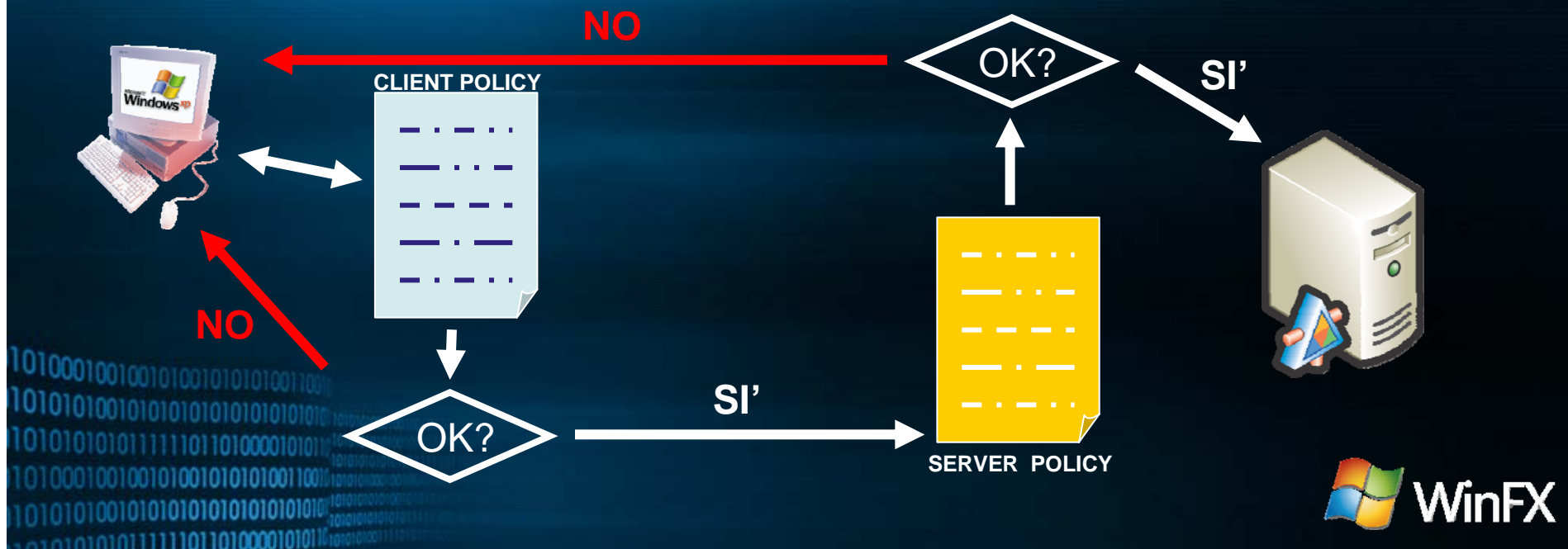
Modello WS-Federation

- IP e RP possono essere all'interno di sistemi informativi diversi



WS-Policy

- Il client e/o il server hanno una lista di regole di sicurezza da rispettare
 - Prima di inviare il messaggio
 - Prima di processarlo “sul serio” alla ricezione



WS-Interoperability

- WS-I organizzazione i cui obiettivi sono:
 - Ottenere l'interoperabilità tra i Web Service
 - Tra piattaforme, applicazioni e linguaggi differenti
 - Promuovere l'utilizzo dei Web Service
 - Sui clienti, le aziende e gli utenti finali
 - Rendere più rapida la produzione di Web Service
- <http://www.ws-i.org/>



WEB SERVICES
INTEROPERABILITY
ORGANIZATION



WS-I Basic Security Profile 1.0

- Bozza (Working Draft) del 29-03-2006 relativo alla sicurezza dei Web Service
 - Interoperabile
- Si occupa di:
 - Sicurezza del trasporto (HTTPS, SSL, TLS)
 - Sicurezza del messaggio (SOAP, WS-Security)
 - Username Token
 - X.509 Certificate Token
 - Binary Security Token
 - Kerberos Token
 - SAML
 - Sicurezza di XML:
 - XML Signature
 - XML Encryption
 - Sicurezza degli allegati a SOAP
- Editors di WS-I:
 - Nortel Networks, Microsoft, IBM, Layer 7

Bindings

	Interopp	Security	Session	Transactions	Duplex	Streaming
BasicHttpBinding	BP 1.1	T				
WSHttpBinding	WS	T S	X	X		
WSDualHttpBinding	WS	T S	X	X	X	
NetTcpBinding	.NET	T S	X	X	X	O
NetNamedPipeBinding	.NET	T S	X	X	X	O
NetMsmqBinding	.NET	T S	X	X		
NetPeerTcpBinding	-	T S			X	
WSFederationHttpBinding	WS	T S	X	X		

T = Transport Security | S = WS-Security | O = One-Way Only



WCF Security Basics

- Authentication
 - Verifica credenziali in base a Claim
- Authorization
 - Host Gate
 - Operation Contract Gate
 - Application Gate
- Confidentiality and Integrity
 - WS-*
- Secure by default
 - Indipendente dal binding

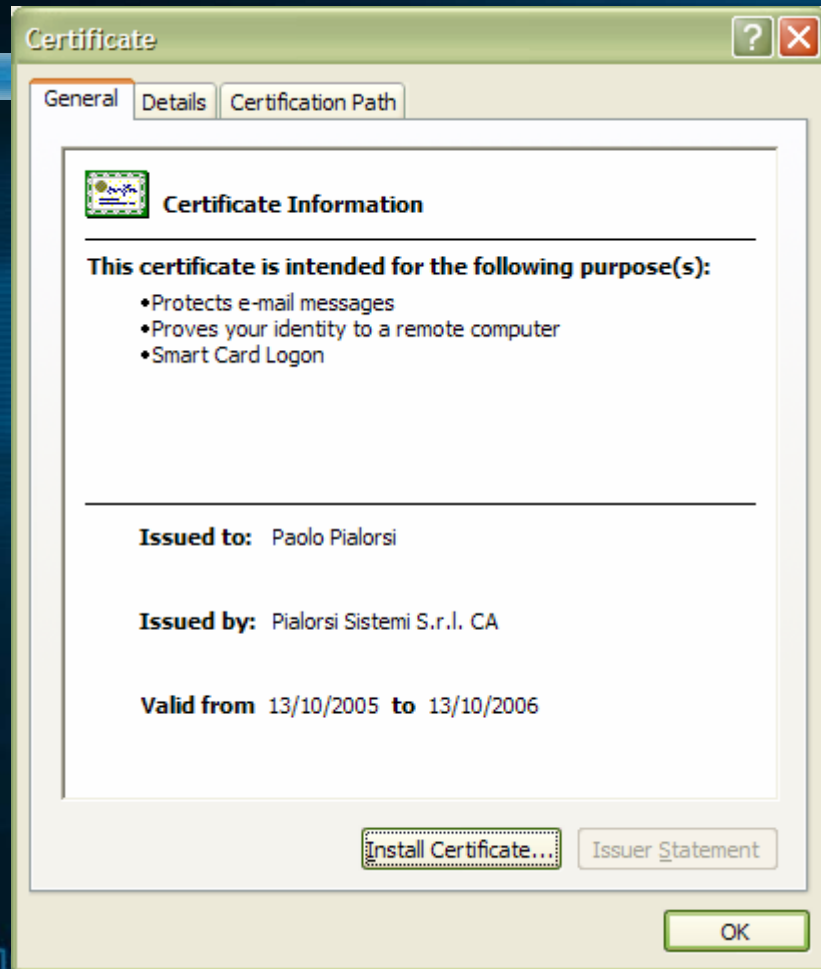
DEMO



CLAIMS

010101010100010010010101010100110011
11001010101010100101010101010101010101
10101010101010101111101101000010101
1010101010100010010010100101010100110011
110010101010101010101010101010101010101

Esempio di Digital Identity



- X.509 Certificate
 - CN=Paolo Pialorsi
 - Issuer=Pialorsi Sistemi CA
 - Valid From=13/10/2005
 - Valid To=13/10/2006
- Subject
 - Paolo Pialorsi
- Issuer
 - Pialorsi Sistemi CA

Sicurezza a livello di trasporto

- Non agisce sul messaggio
- Si basa sul trasporto
 - HTTPS (SSL/TLS)
 - VPN
 - IPSec
 - Ecc.
- Vantaggi prestazionali
 - No overhead per WCF engine
- Svantaggi sul fronte della estendibilità
- Non è un approccio Service Oriented



DEMO

TRANSPORT SECURITY

010101010100010010010101010100110011
11001010101010100101010101010101010101
10101010101010101111101101000010101
1010101010100010010010100101010100110011
110010101010101010101010101010101010101

Sicurezza a livello di messaggio (1/2)

- Utilizza WS-* sul messaggio
 - WS-Security
- Fornisce:
 - Integrità
 - Riservatezza
 - Autenticazione
- Può lavorare su porzioni di messaggio
- Sfrutta il concetto di Claim

Sicurezza a livello di messaggio (2/2)

- Infrastruttura estendibile
 - Custom Tokens
 - Custom Claims/Validators
- Indipendente dal trasporto
 - Supporta più “hop” del messaggio (SOAP intermediaries)
- Molto Service Oriented
- A volte ancora “in divenire”



DEMO

MESSAGE SECURITY

010101010100010010010101010100110011
10010101010101001010101010101010101010
101010101010101011111011010000101011
1010101010100010010010100101010100110011
100101010101010101010101010101010101010

Sicurezza mista

- Integrità e riservatezza tramite il trasporto
 - HTTPS (SSL/TLS)
 - VPN
 - IPSec
 - Ecc.
- Autenticazione tramite WS-* sul messaggio
 - WS-Security Tokens
- Utilizza i Claim
- Estendibile solo sui Token
- Spesso la virtù sta nel mezzo ☺ ...

Credenziali

- Windows e/o Kerberos
 - DOMAIN\Username
- UsernameToken
 - Username + Password
- X.509 Certificate
 - CN=DevLeap; Issuer=DevLeap CA; ecc.

UsernameToken Validation

- Windows Machine Domain
 - Utente di macchina o dominio
- Membership API
 - Database utenti di ASP.NET
- Custom Membership Provider
 - Database utenti applicativo via Membership
- Custom UsernameValidator
 - Database utenti applicativo via custom code



DEMO

USERNAMETOKEN CUSTOM

010101010100010010010101010100110011
11001010101010100101010101010101010101
101010101010101011111011010000101011
10101010101000100100101001010100110011
110010101010101010101010101010101010101



DEMO

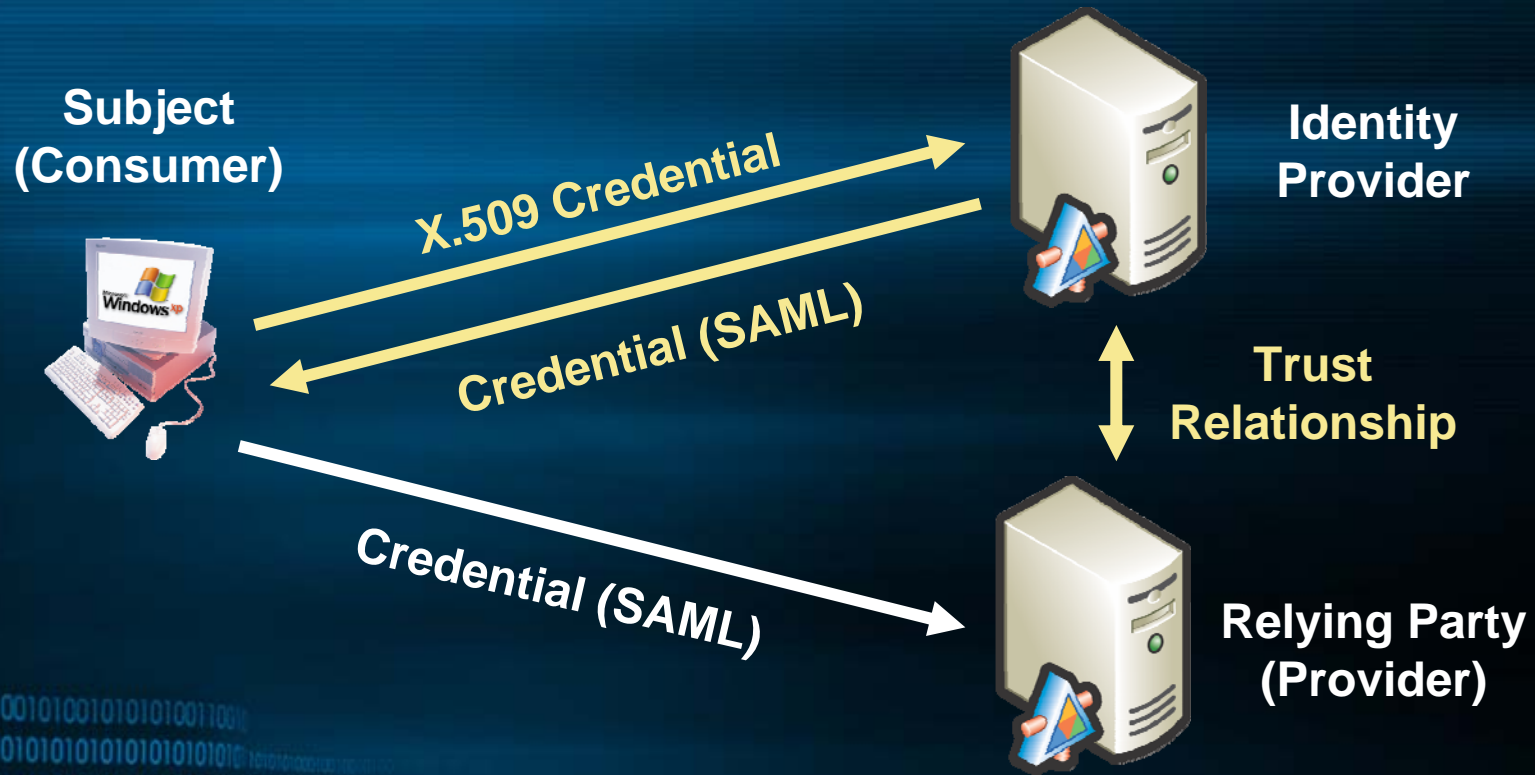
SECURE CONVERSATION

01010101010001001001010101010011001
1001010101010100101010101010101010101
10101010101010101111101101000010101
1010101010100010010010100101010011001
1001010101010101010101010101010101010

WS-Federation

- Prevede una “raccomandazione”
 - Da parte di qualcuno di fidato
- Flusso logico
 - Una trusting authority mi valida
 - Ottengo un token
 - Mi presento al provider usando il token
- Faciliterà la comunicazione tra piattaforme

Modello WS-Federation



Host Gate

- Utilizza le policy di autorizzazione a livello di server
- Filtri IP (IIS o Firewall)
- Access Control List
 - File System
 - IIS
- ASP.NET Authorization

Operation Contract Gate

- Sfrutta System.Security.Permission
 - PermissionPrincipal
- Richiede impersonation
 - IIdentity e IPrincipal
 - Eventualmente Custom
- Sicurezza dichiarativa .NET Framework

Application Gate

- Sfrutta System.Security.Permission
 - Classi *Permission
 - Anche custom!
- Richiede impersonation
 - IIdentity e IPrincipal
- Sicurezza imperativa .NET Framework

InfoCard (1/2)

- Meccanismo di autenticazione
- Selezione delle credenziali
 - Da un portafoglio di credenziali per l'utente
- Indipendente dall'infrastruttura tecnologica
- Si basa su WS-Trust (interoperabile)

InfoCard (2/2)

- Active Directory v.next supporterà InfoCards
- Annunciato il supporto extra-Windows
 - Linux, Unix, Apache, ecc.
- Supporta SAML 1.1

Come funziona?



Protocolli di base

InfoCard



WS-MetadataExchange,
WS-Security,
WS-Trust



WS-MetadataExchange,
WS-Security



Autenticarsi verso un Identity Provider

- La definizione di InfoCard supporta
 - UsernameToken
 - X.509 Certificate
 - Kerberos
 - Self-issued InfoCard

Ulteriori approfondimenti

- Siti Web a proposito di WCF:
 - <http://msdn.microsoft.com/webservices/>
 - <http://windowscommunication.net/>
- DevLeap:
 - <http://www.devleap.com/>

Microsoft®

Your potential. Our passion.™



WinFX