Interoperability & Federation con ADFS 2.0

Mario Fontana
Senior Software Architect - Security
Developer & Platform Group - Microsoft
http://blogs.msdn.com/mariofontana

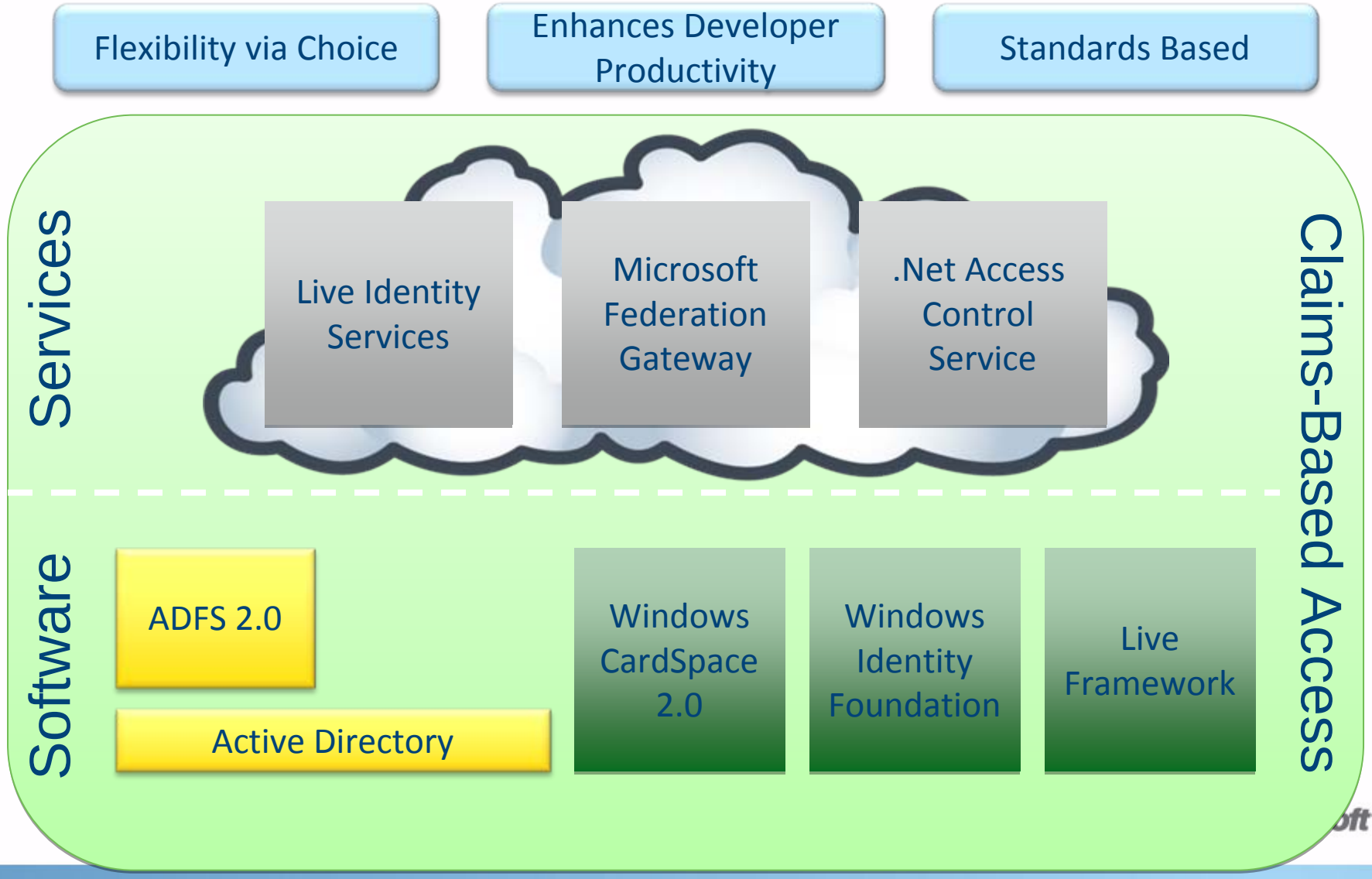
International Association of Software Architects
IASA Chapter Italy : Founder & CEO

Microsoft

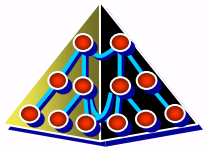
Active Directory Federation Services 2

- Active Directory come IDP (anche) per le applicazioni
  - Identity & Federation Provider
  - Evoluzione di ADFS presente in Windows Server 2003 R2 e successivi
- Basato su standard
  - WS-* e SAML 2.0 Protocol
  - Token SAML 1.1 e Token SAML 2.0
- Federation Trust Manager
  - Automatizza il trust management via metadata
- Provider per Information Cards
  - Per CardSpace e altri Identity Selectors

Microsoft Identity Software + Services

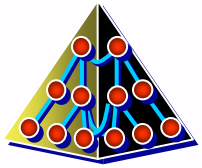


ADFS 2.0



ADDS

Custom Attribute Store



Active Directory

Active Directory
Federation Services 2.0

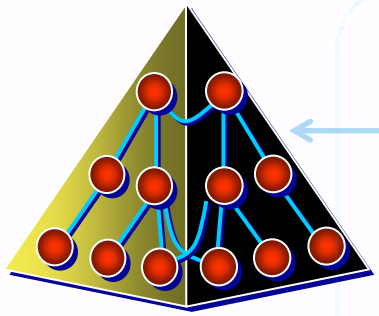
trust

Client

Relying Party

Microsoft

Federation



AD FS 2.0

trust

AD FS 2.0

- Shibboleth
- ICAR-INF3
- OpenSSO
- CA SM
-Novell Access Manager
-…

trust

5. Authenticate

3. Home realm discovery

4. Redirect to STS

1. Attempt access

2. Redirect to STS

Utente

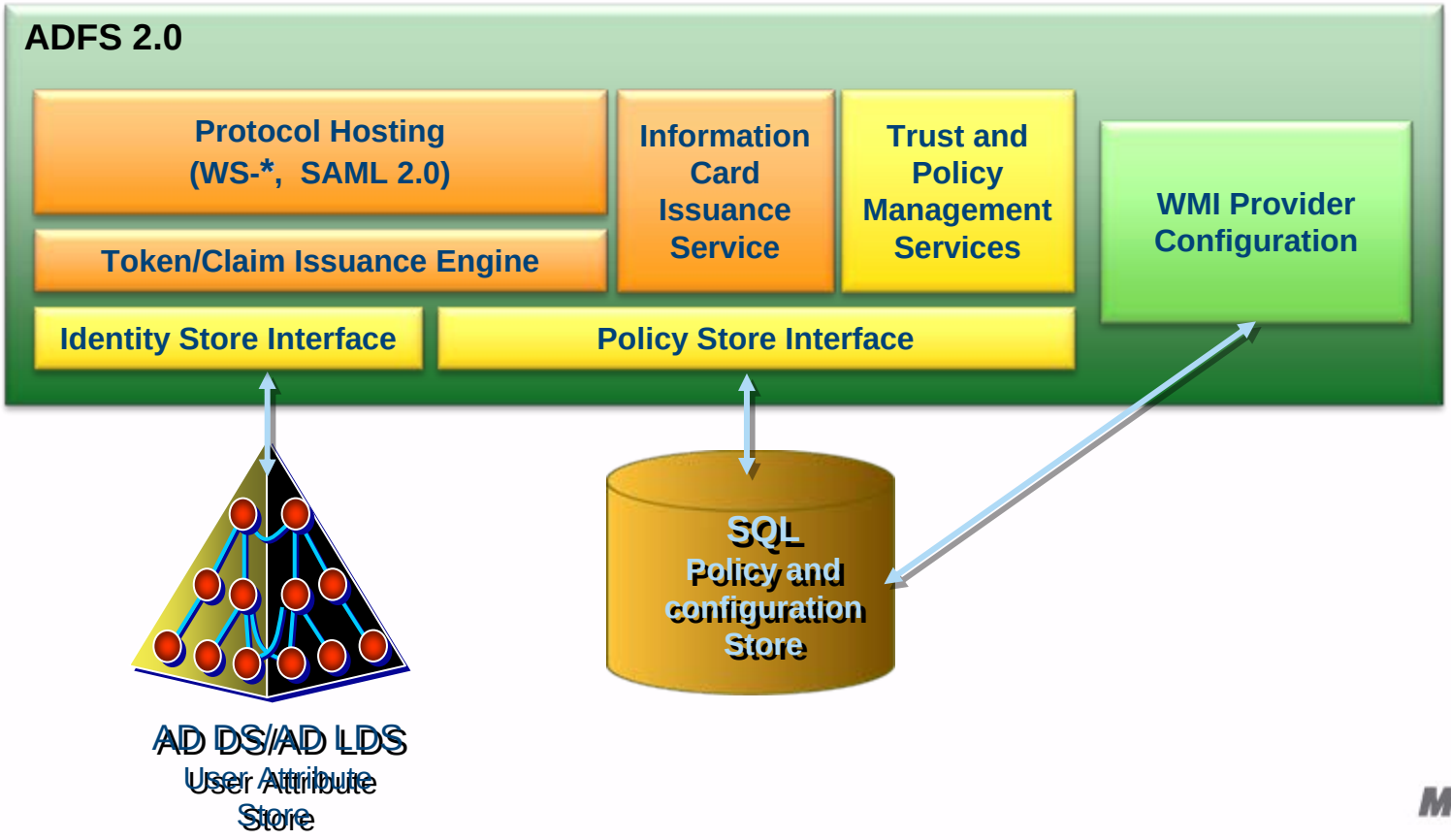
Applicazione

Claims-Framework

Relying Party

Microsoft

ADFS 2.0 Architecture



Protocolli

- ADFS 2.0 supporta entrambte le specifiche standard di riferimento :
  - WS-*
    - WS-Security, WS-Trust, WS-Federation (WSFED)
      - Sviluppata originariamente da : BEA Systems, BMC Software, CA, Inc., IBM, Layer 7 Technologies, Microsoft, Novell, Ping Identity, e VeriSign.
      - **Standard OASIS**
  - SAML 2.0 Protocol
    - Convergenza tra SAML 1.1 Protocol, Liberty ID-FF1.2 e Shibboleth
    - **Standard OASIS**

Supporto ai protocolli WS-*

	AD FS1	ADFS 2.0
WS-Federation 1.0 (Passive Requestor Interop Profile)	Y	Y
WS-Federation 1.2 (Min Passive Requestor Subset)	n/a	Y
▪ POST (push) Binding		Y
▪ wresultptr (pull) Binding		Y
▪ Home Realm Discovery service		Y
WS-Trust 1.3 (aka Active Requestor Profile)	n/a	Y
▪ Issue		Y
▪ Issue “OnBehalfOf” (proxy support)		Y
▪ Issue “ActAs” (identity delegation)		Y
▪ Renew		Y
▪ Validate		Y
WS-SecurityPolicy 1.2	n/a	Y

Supporto al protocollo SAML 2.0

	AD FS1	ADFS 2.0
SAML 1.0/1.1 Web SSO Protocol	N	N
SAML 2.0 Web SSSO Protocols	n/a	Y
▪ IdP Lite & SP Lite Operational Modes		Y
• Web SSO, <AuthnRequest>, HTTP redirect		Y
• Web SSO, <Response>, HTTP POST		Y
• Identity Provider Discovery (cookie)		Y
• Web SSO, <Response>, HTTP Artifact		Y
• Artifact Resolution, SOAP		Y
• Single Logout (IdP-initiated) – HTTP redirect		Y
• Single Logout (SP-initiated) – HTTP redirect		Y
• Enhanced Client/Proxy SSO, PAOS (*)		Y
▪ GSA Profile (LA harmonized e-Gov Profile)		Y

Microsoft

SAML Token Support

	AD FS1	ADFS 2.0
SAML 1.1 Tokens	Y	Y
▪ Authentication & Attribute Statements	Y	Y
▪ Signed tokens	Y	Y
▪ Encrypted tokens	N	Y
SAML 2.0 tokens	n/a	Y
▪ Authentication & Attribute Statements		Y
▪ Extensible claim type (any URI)		Y
▪ Signed tokens		Y
▪ Encrypted tokens		Y
▪ Proof tokens (symmetric/asymmetric keys)		Y

SAML 2.0 P Interoperability

- 2 Use Cases:
  - OASIS SAML 2.0 IdP Lite and SP Lite
  - US Government GSA profile
- SAML IdP interop workshops
  - IBM
  - Ping Identity
  - CA
  - Sun Microsystem
  - Novell
  - Shibboleth 2.0
    - l' Università di Washington
    - Scott Cantor dell' Ohio State University
- Include I ruoli IdP e SP
- Whitepapers disponibili.

Un primo caso in Italia di interoperabilità via SAML 2.0

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

UNIBOmagazine

Home | Notizie | Eventi | Attualità | Università | Iniziative | Libri | Sport | Fotoracconti

Sei in: Home ¬ Università ¬ 2009 ¬ agosto ¬ giovedì 06 ¬ Geneve

Da Unibo l'accesso ai servizi di e-goverment di Lepida

6 agosto 2009
Autore: Monica Lacoppola

Grazie alle credenziali Unibo sarà possibile accedere a siti e servizi delle pubbliche amministrazioni regionali che fanno parte del sistema federato di Lepida. Primo risultato raggiunto per il progetto Alma Federation, cofinanziato nell'ambito di Campus Digitali il programma ICT4Univeristy promosso dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio.

Test superato per il **nuovo prodotto Microsoft "Geneva"** che consente di far dialogare i sistemi di autenticazione basati su Microsoft Active Directory dell'Università di Bologna con quelli di **Lepida Spa**, in specifico con il sistema di **autenticazione federata fedERa**, basato sullo **standard internazionale SAML 2.0** e implementazione del **sistema di identità federata ICAR**. In pratica, gli oltre centomila utenti (studenti, docenti, personale tecnico-amministrativo e collaboratori) che dispongono di credenziali di accesso al sistema Unibo potranno utilizzarle per accedere ai siti e ai servizi delle pubbliche amministrazioni che fanno parte del sistema federato di Lepida.

Grazie ad **un accordo tra Università di Bologna e Lepida e con la collaborazione di Cefriel e Microsoft è stata infatti sperimentata con successo l'interoperabilità fra il sistema fedERa** e un nuovo middleware di federazione realizzato da Microsoft, appunto "Geneva Server" raggiungendo l'obiettivo, di reciproco interesse per Lepida (e quindi per tutti gli enti "federati") e per l'Ateneo, di consentire agli utenti autenticati dall'Università di Bologna l'accesso ai servizi di e-government offerti dagli enti dell'Emilia-Romagna utilizzando le credenziali fornite dall'Università e senza bisogno di crearne di nuove.

Un altro scenario di interesse che potrà essere sperimentato in futuro prevede la **possibilità di integrare nel sistema dell'Università di Bologna gli Identity Provider degli enti dell'Emilia-Romagna**, così da rendere disponibili i servizi dell'Università ai collaboratori della pubblica amministrazione regionale e ai cittadini in genere autenticati dagli enti.

Harmonized Federation Metadata per WS-FED e SAML 2.0P

- Automazione della configurazione degli IP e SP con la pubblicazione dei federation metadata tramite standard.
- WS-Federation è stato modificato per integrare una dipendenza normativa con il *SAML 2.0 federation metadata document structure*.
  - The WS-Federation specification defines extensions for web services constructs (such as Endpoint References) that are required for WS-* protocols.
- Presente (anche in Shibboleth)
  - The SAML 2.0 standard includes the *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0* specification [Samlv2Meta] that is devoted to standardization of a federation metadata format.

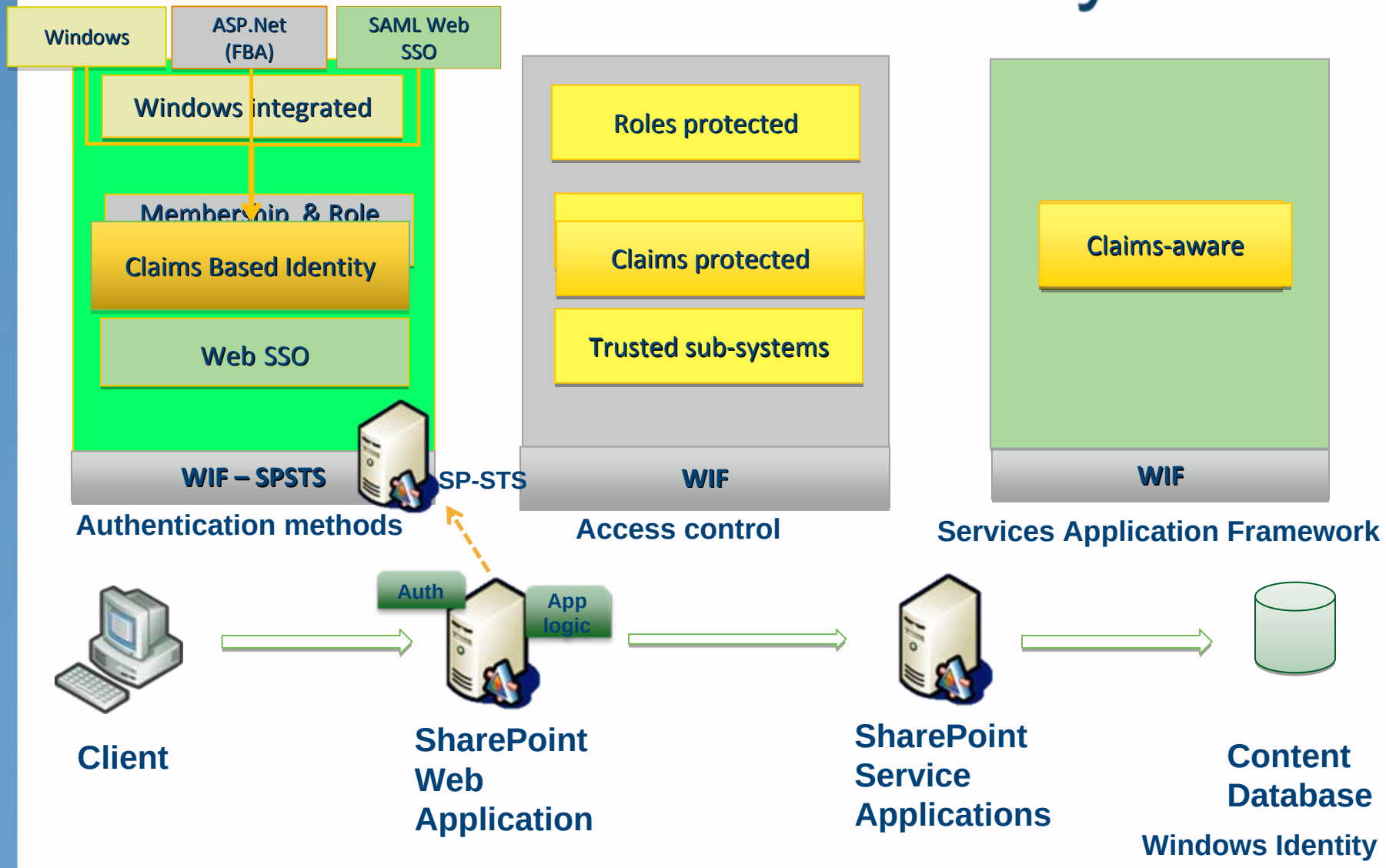
Microsoft

Windows Identity Foundation (WIF)

- Claims programming model
  - Claims Object Model integrato con le .NET identity API
  - Unico programming model per ASP.NET & WCF
  - Unico programming model per on-premises & cloud
  - Config driven
- Configurazione tramite Tools
- Framework per lo sviluppo di custom STS (IDP)

- ADFS 2.0 è stato sviluppato con WIF!
  - …e non solo ADFS 2.0!

SharePoint 2007 – Identity Flow



Microsoft

References

- Mario.fontana@microsoft.com
- IASA Chapter Italy : http://www.iasahome.org/web/italy/home
- Interoperability : http://www.moreinterop.com/
- Interop Whitepapers : http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=9eb1f3c7-84da-40eb-b9aa-44724c98e026