Trusting XBRL: Using the Liberty Web Services Framework to Secure and Authenticate XBRL Documents

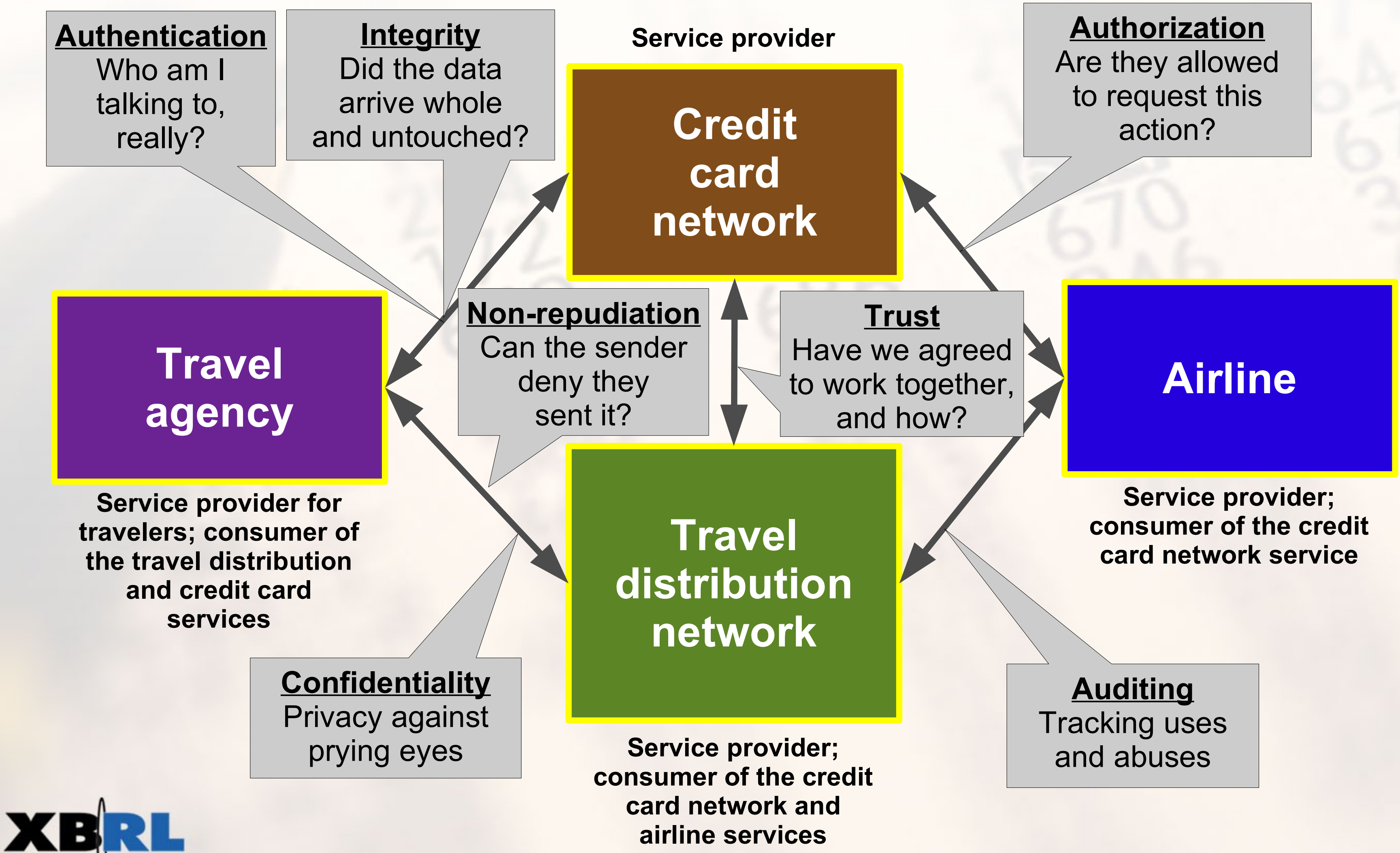
Farrukh Najmi and Eve Maler
farrukh.najmi@sun.com, eve.maler@sun.com
Sun Microsystems, Inc.

Goals for today's talk

- Discuss modern technologies for security and identity
  - In light of the special challenges and opportunities presented by XML and web services
  - Ultimately focusing our attention on the Liberty Identity Web Services Framework (ID-WSF)
- Provide food for thought on how you can take advantage of these technologies in the near term

The Problem Space

Web services in general have all the classic security requirements...



Authentication
Who am I talking to, really?

Integrity
Did the data arrive whole and untouched?

Service provider

Credit card network

Authorization
Are they allowed to request this action?

Travel agency

Service provider for travelers; consumer of the travel distribution and credit card services

Non-repudiation
Can the sender deny they sent it?

Trust
Have we agreed to work together, and how?

Airline

Service provider; consumer of the credit card network service

Travel distribution network

Service provider; consumer of the credit card network and airline services

Confidentiality
Privacy against prying eyes

Auditing
Tracking uses and abuses

XBRL
eXtensible Business Reporting Language

...and some unique opportunities...

- Security services can increase security-by-design
  - As they become more available “horizontally” through a service-oriented architecture
- XML increases the granularity of security operations on data
  - Signing precisely the data you're willing to make a claim about
  - Encrypting precisely the data that must be kept private
  - Marshalling security context and identity data into an XML form

...but also some unique challenges

- Service interfaces and HTTP ports tend to be more exposed to abuse
- SOAP intermediaries: men in the middle?
- As more services are outsourced, security domains must be routinely crossed
- Semantic mismatches between security models of different domains
    - How to propagate security context (such as for SSO)?
    - How to match up roles in distributed authorization?

Not to mention the more classic threats

XBRL's special requirements and challenges

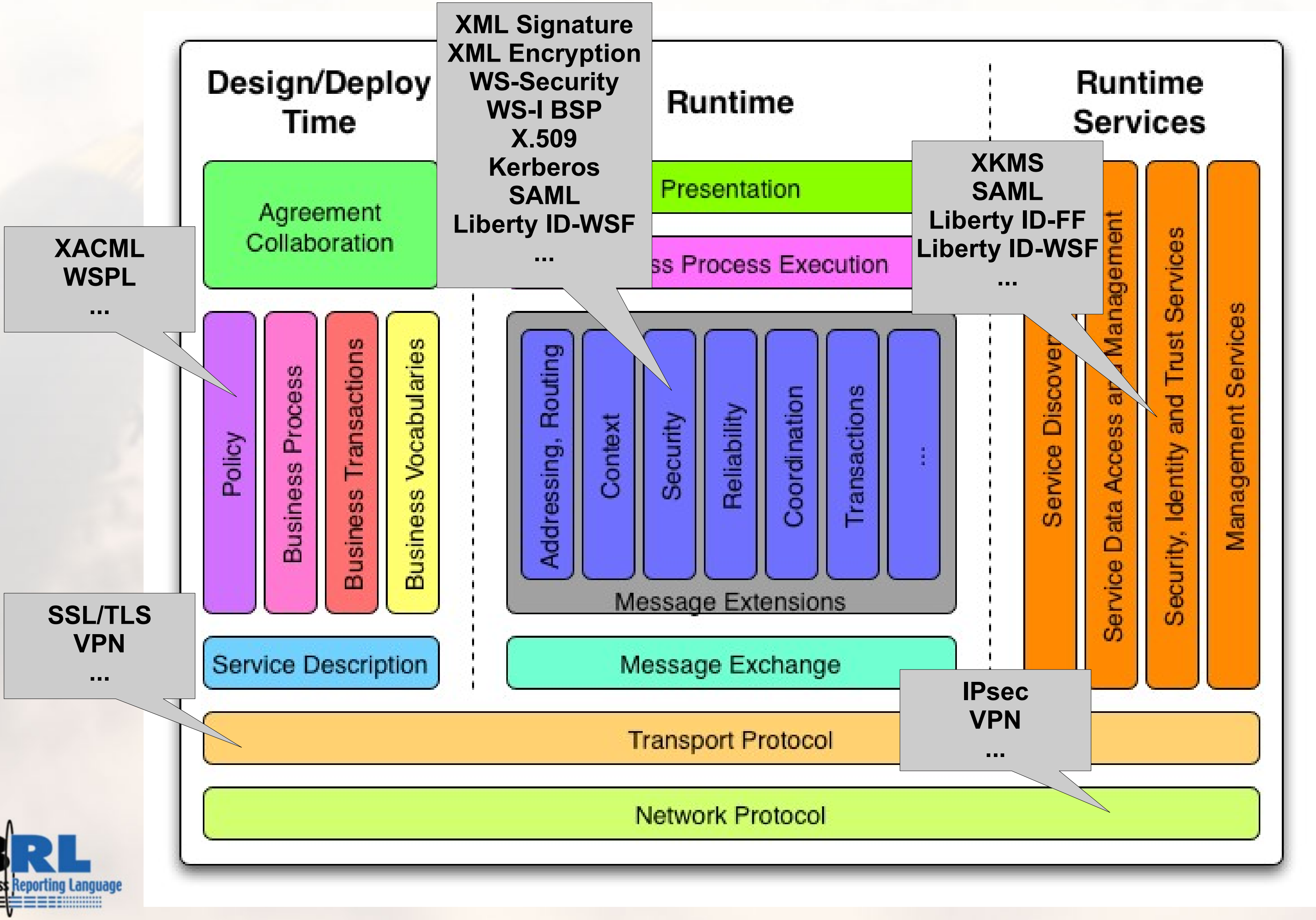
- Ensuring that the XBRL representation is amenable to electronic security technologies
  - XBRL GL would ease some difficulties here
- Aggregating authenticated data from various sources
- Multiple parties making a variety of assurances about the same report
- Logging the passage of data through various hands
- Privacy and confidentiality of selected data
- Access control early in the (increasingly speedy) lifecycle; “B-to-anonymous” pattern later

One vision of XBRL security nirvana

- Access is controlled and logged throughout report creation
- On viewing an XBRL-based report, all assurances associated with the content are made available for browsing in a graphical manner
- Any view of the report data is able to extract the relevant security assurances

The Solution Space

Web services technologies from 5,000 feet up



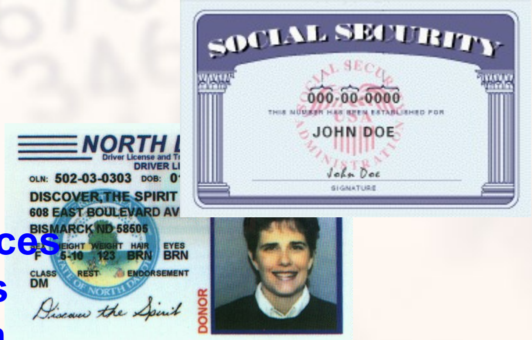
XBRL eXtensible Business Reporting Language

The notion of identity is critical

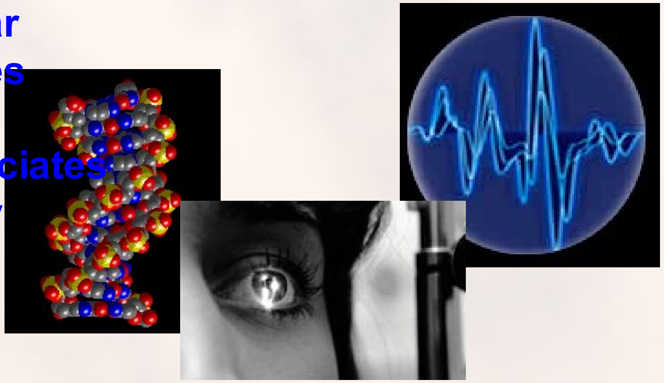
- Web services are ultimately performed on behalf of things with identities
  - Not just humans
- Identities can be managed with web services
- Identity and web services are interdependent
  - In all but the most trivial cases

Customer name	John Smith
Email alias	jsmith2@freemail.com
User ID	js@eng.example.com

Credit card number
Social security number
Driver's license
Passport
Retinal scan
DNA

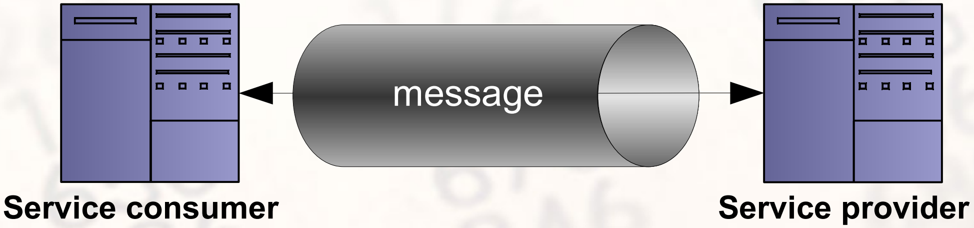


Entertainment preferences
Notification preferences
Employee authorization
Business calendar
Dining preferences
Affinity program
Friends and associates
Education history
Medical history
Financial assets
...

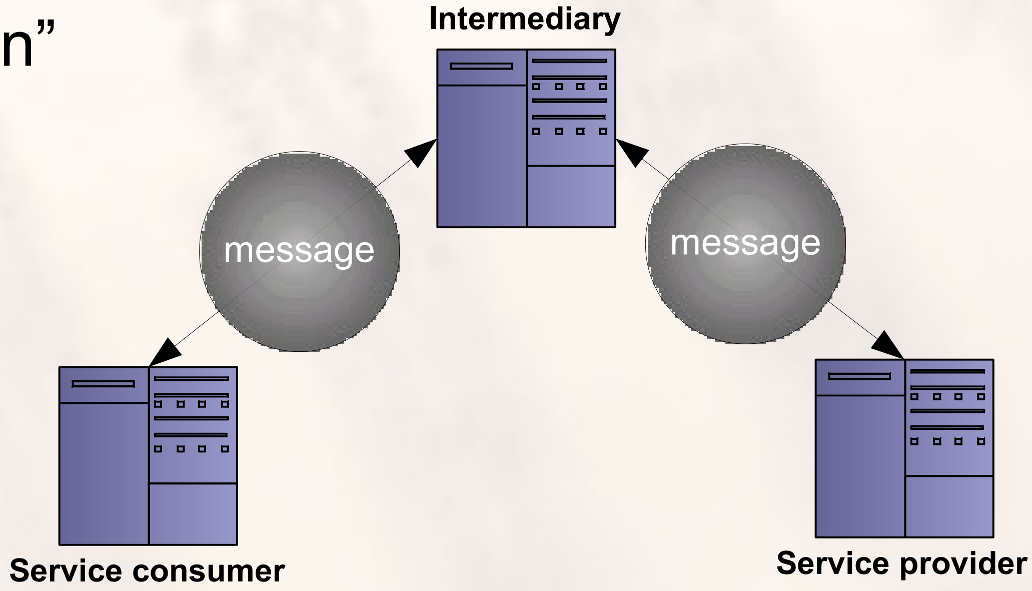


Transport-layer vs. message-layer security

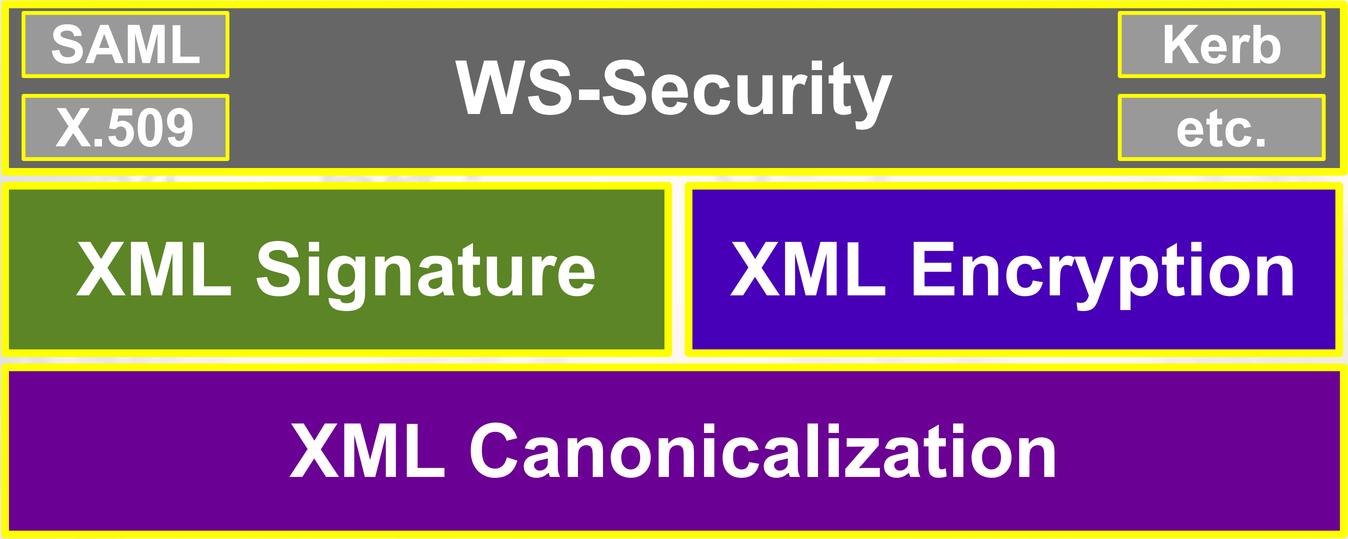
- Well-understood
- Limited to pairwise connections; not end-to-end
- Doesn't distinguish individual pieces of data
- Covers data “in motion” but not “at rest”



- Flexible and fine-granularity
- Newer on the scene
- More moving parts



Message security rides on top of generic XML security



SAML

X.509

WS-Security

Kerb

etc.

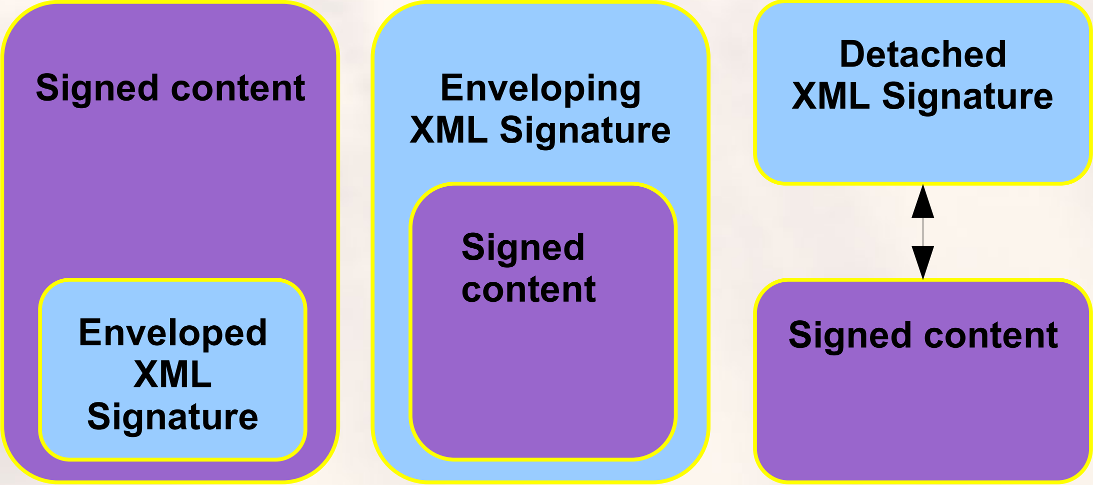
XML Signature

XML Encryption

XML Canonicalization

XML Signature: fine-grained data origin authentication

- XML vocabulary and process from W3C and IETF for digitally signing whole or partial XML documents (or non-XML content) and validating signatures
- **<ds:KeyInfo>** identifies the relevant key
  - Reused (profiled) in many other specs
- XML Canonicalization (C14N) normalizes data



Some potential applications of XML-based signing to XBRL

- Company management:
  - “This is the report as it was published”
  - “This one fact came out of that published report”
- Auditor:
  - “This report is true”
- Regulator or stock exchange:
  - “This report was lodged with us at the indicated time”

XML Encryption: fine-grained confidentiality

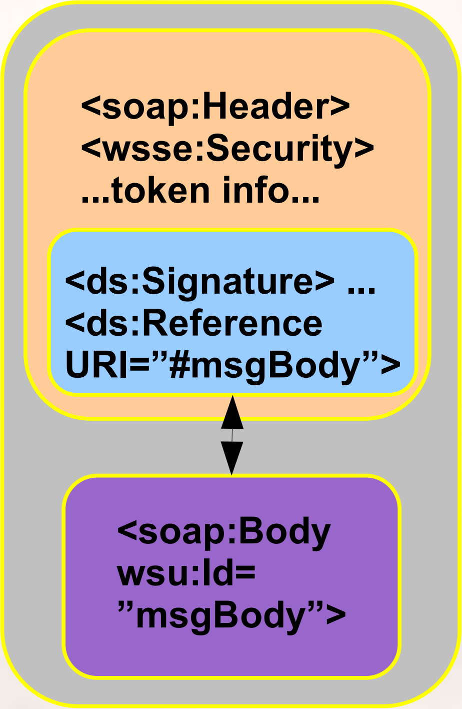
- XML vocabulary and process from W3C for encrypting and decrypting a whole or partial XML document
- C14N used here as well

```
<InventoryData>
 <Date>…</Date>
 <Products>
  <Product Amt="3">
  Chia Head</Product>
  <Product …>…</Product>
  …
 </Products>
</InventoryData>
```

```
<InventoryData>
 <Date>…</Date>
 <EncryptedData …>
  <CipherData>
   <CipherValue>
   …SKFWw5F34=…</CipherValue>
  </CipherData>
 </EncryptedData>
</InventoryData>
```

WS-Security and BSP: the basics of SOAP messaging security

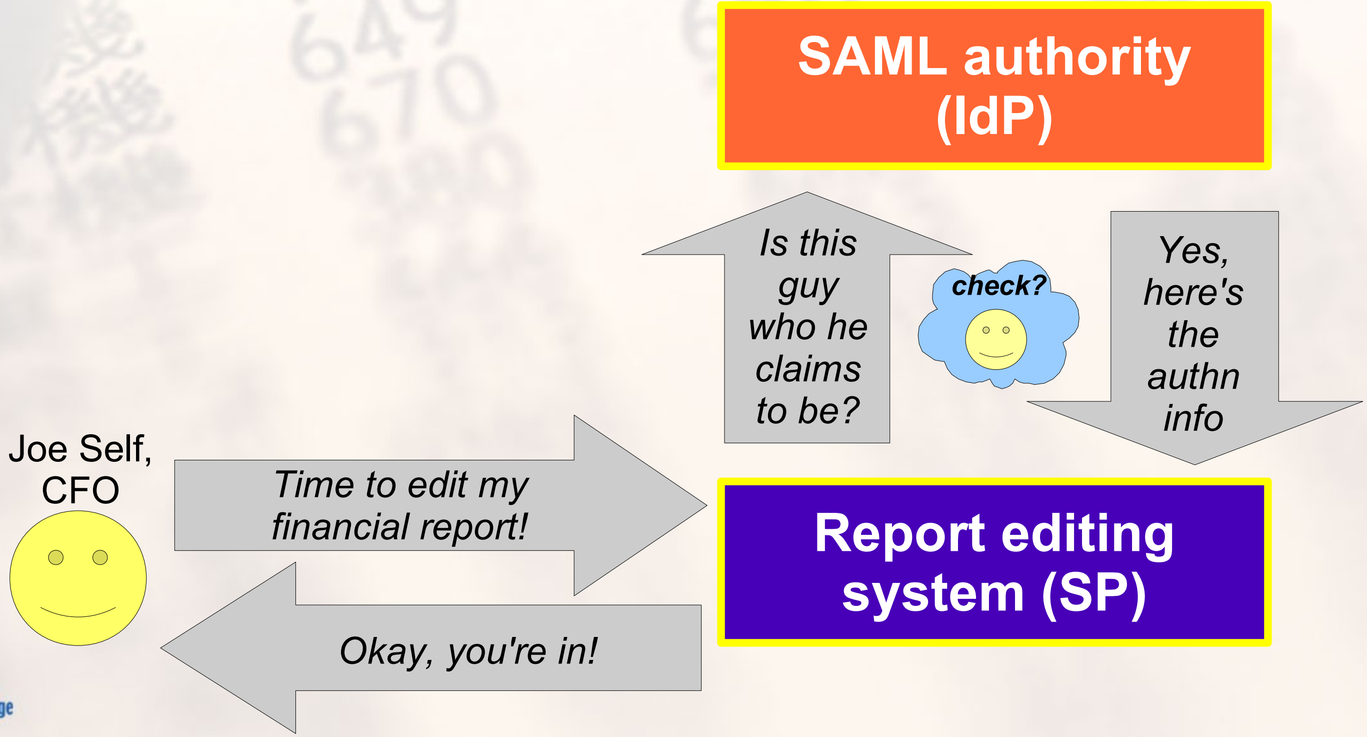
- WS-Security from OASIS defines the **<wsse:Security>** SOAP header and how to use it with XML Signature, XML Encryption, and a variety of ***security tokens***
  - Username, X.509 certs,Kerberos tickets, SAML assertions, ...
  - A timestamping feature is also defined
- Basic Security Profile from WS-I further constrains WS-Security and SSL/TLS for interoperability



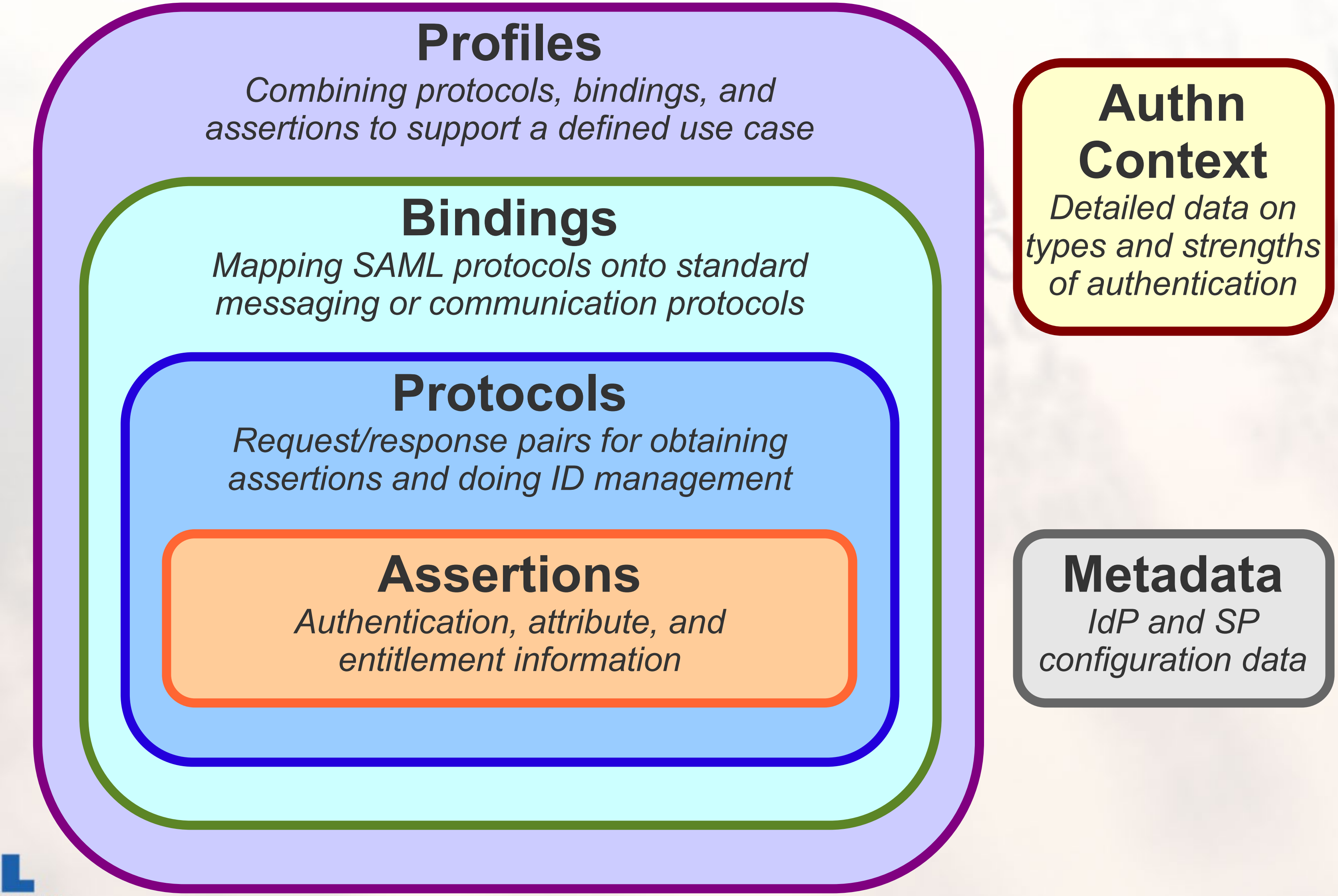
Technologies that Specialize in Identity

SAML: the universal solvent of security and identity information

- SAML from OASIS is a framework for conveying security information about subjects
- In many scenarios, ***identity providers*** serve SAML security ***assertions*** to ***service providers***


SAML authority (IdP)
Is this guy who he claims to be?
check?
Yes, here's the authn info
Joe Self, CFO
Time to edit my financial report!
Report editing system (SP)
Okay, you're in!

SAML piece-parts



Profiles

Combining protocols, bindings, and assertions to support a defined use case

Bindings

Mapping SAML protocols onto standard messaging or communication protocols

Protocols

Request/response pairs for obtaining assertions and doing ID management

Assertions

Authentication, attribute, and entitlement information

Authn Context

Detailed data on types and strengths of authentication

Metadata

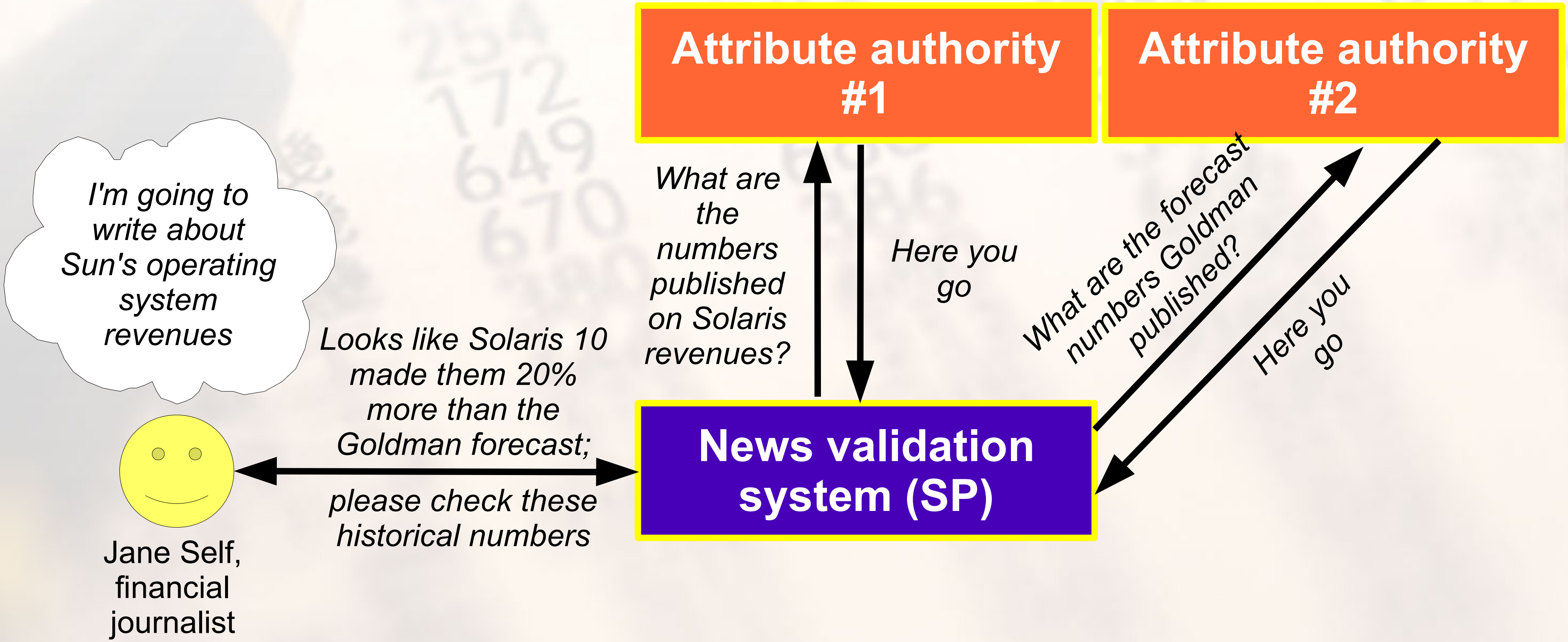
IdP and SP configuration data

SAML assertions can be exchanged for a variety of purposes

- Single sign-on (SSO) and attribute-based authorization
- Mapping identities across systems (identity federation) for better customization and privacy
- Protecting web service messages, in combination with WS-Security
- Industry groups and vendors have defined their own SAML extensions and profiles
    - SAML is highly extensible but demands strict accounting of all new uses, for interoperability
    - The Liberty Alliance profiled SAML for its Identity Federation Framework (ID-FF), now converged into SAML V2.0

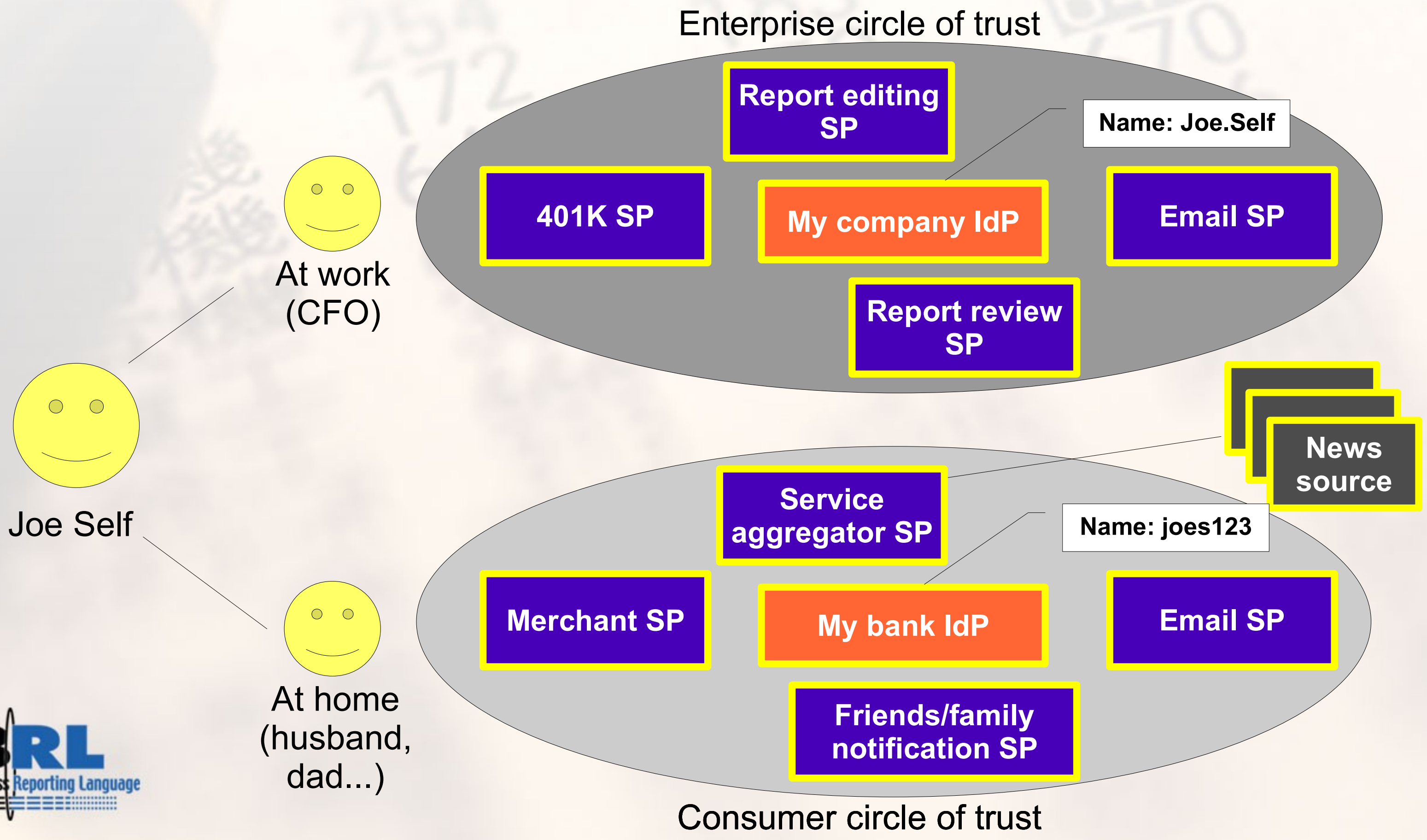
A potential application of SAML to XBRL

- Not (necessarily) for access control, but for ascertaining the claims made in report data

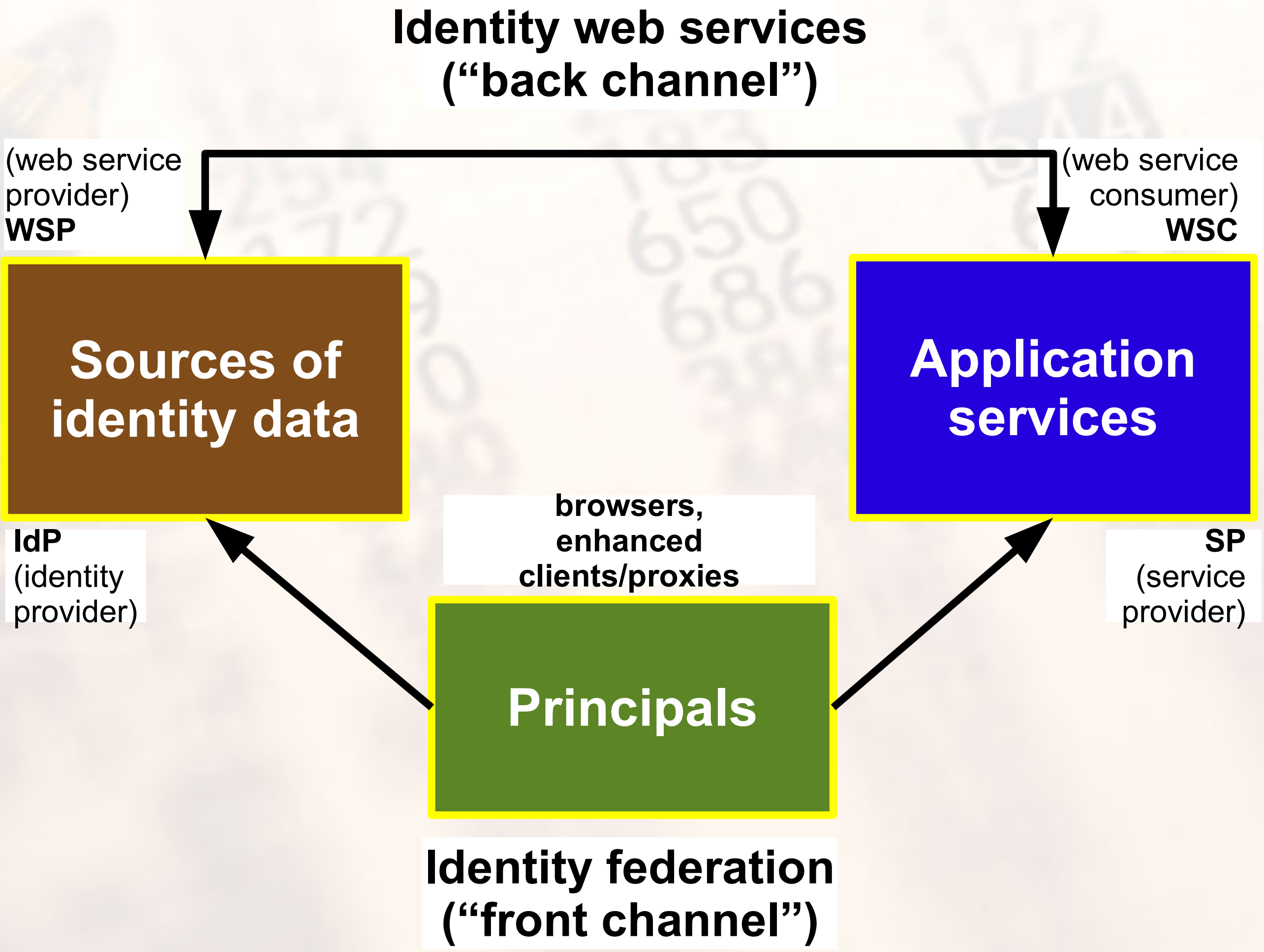

Attribute authority #1
Attribute authority #2
I'm going to write about Sun's operating system revenues
Looks like Solaris 10 made them 20% more than the Goldman forecast;
please check these historical numbers
What are the numbers published on Solaris revenues?
Here you go
What are the forecast numbers Goldman published?
Here you go
News validation system (SP)
Jane Self, financial journalist

Liberty: pervasive identity throughout web applications and web services

- Liberty provides for ***circles of trust*** within which identity info can be shared, while preserving privacy across services
  - Technical solutions + business and legal guidelines



High-level architectural model



Identity web services
(“back channel”)

(web service provider)
WSP

(web service consumer)
WSC

Sources of identity data

Application services

IdP
(identity provider)

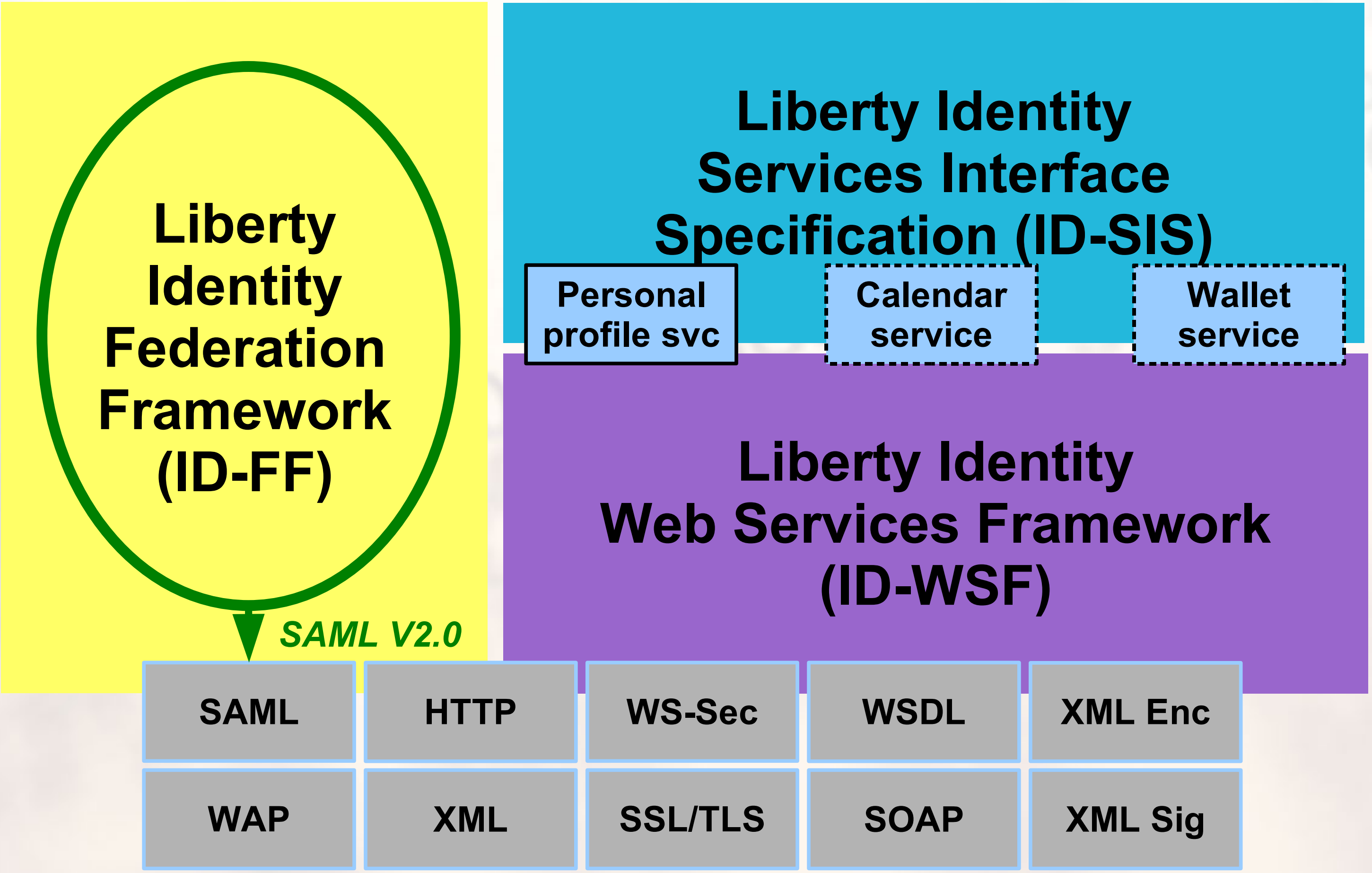
SP
(service provider)

browsers, enhanced clients/proxies

Principals

Identity federation
(“front channel”)

Liberty specification piece-parts



Liberty Identity Federation Framework (ID-FF)

SAML V2.0

Liberty Identity Services Interface Specification (ID-SIS)

Personal profile svc

Calendar service

Wallet service

Liberty Identity Web Services Framework (ID-WSF)

SAML

HTTP

WS-Sec

WSDL

XML Enc

WAP

XML

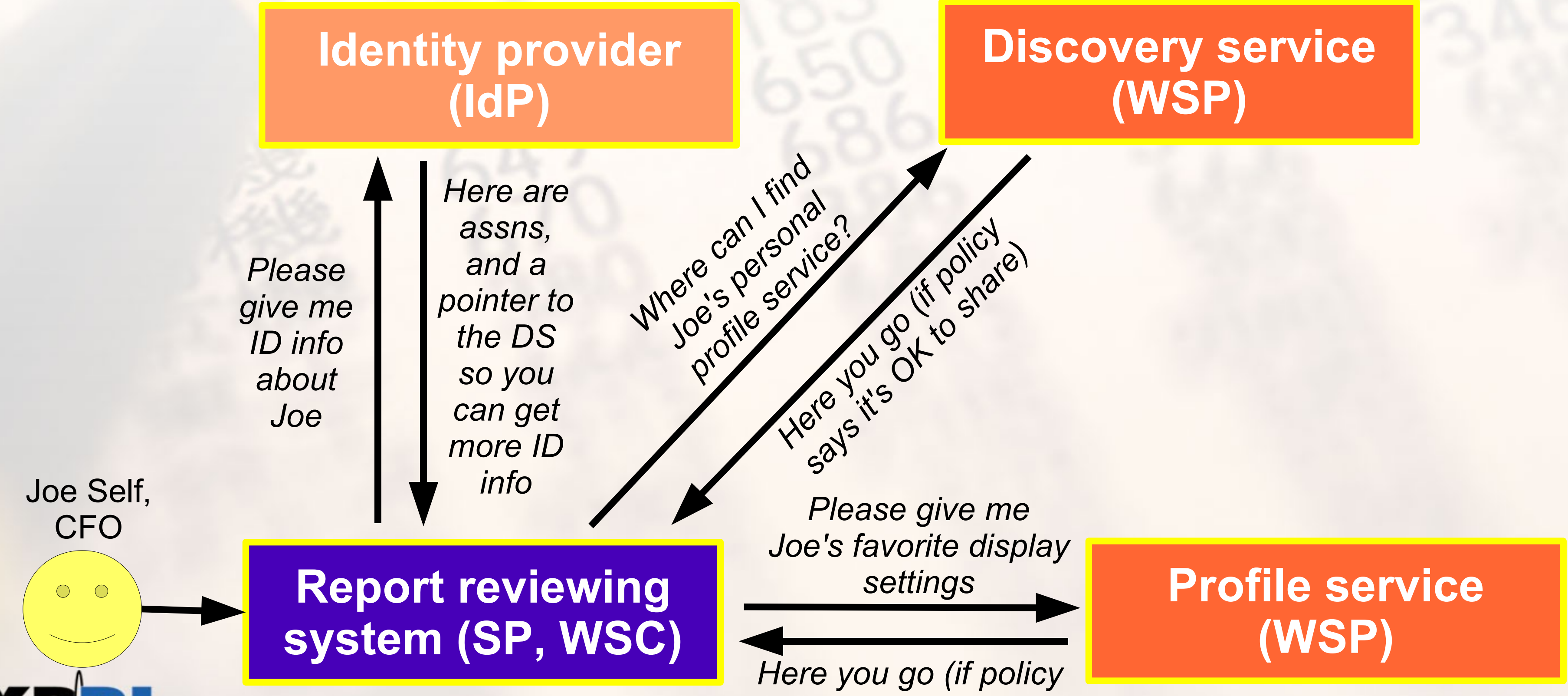
SSL/TLS

SOAP

XML Sig

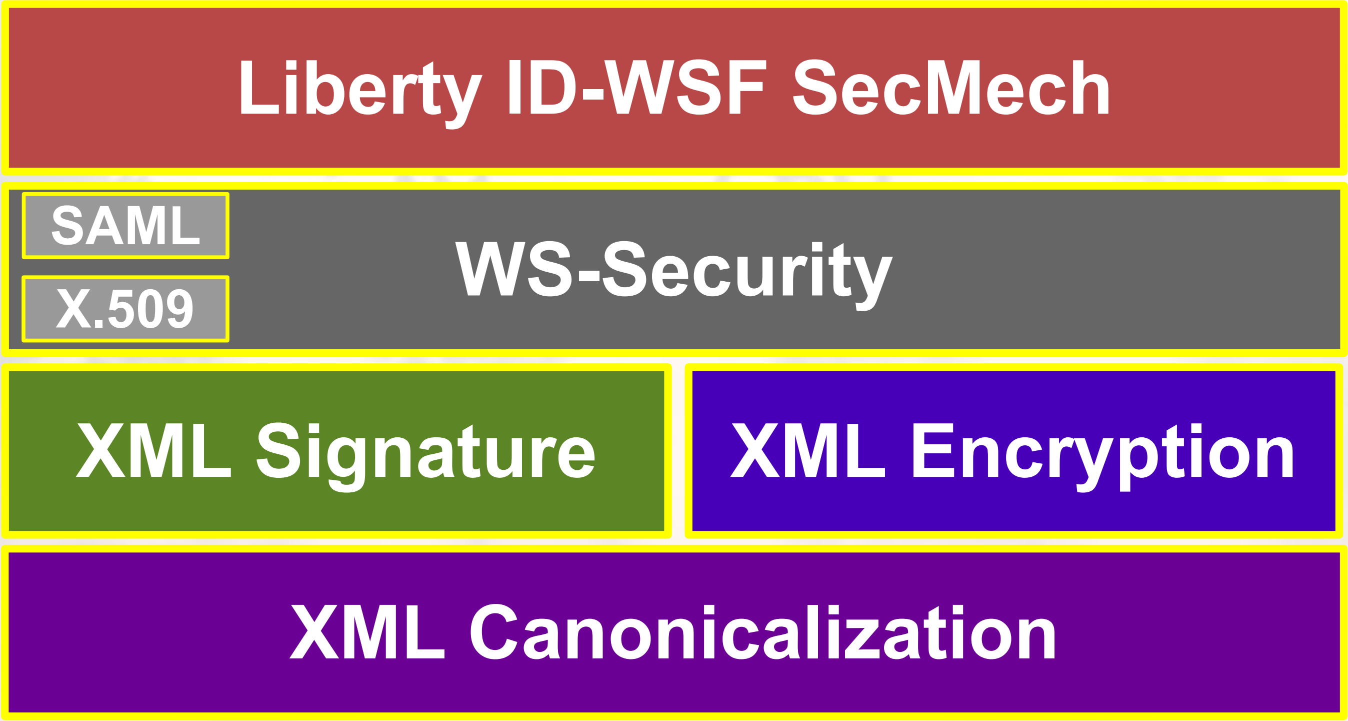
Liberty ID-WSF: privacy-protected, secure identity for web services

- Framework for securing, and propagating identity through, web services interactions



Identity provider (IdP)
Discovery service (WSP)
Please give me ID info about Joe
Here are assns, and a pointer to the DS so you can get more ID info
Where can I find Joe's personal profile service?
Here you go (if policy says it's OK to share)
Joe Self, CFO
Report reviewing system (SP, WSC)
Please give me Joe's favorite display settings
Here you go (if policy says it's OK to share)
Profile service (WSP)

Liberty ID-WSF Security Mechanisms: secure identity services messaging



Food for Thought

First steps on the path to XBRL security nirvana: some questions to ask

- What security protection should apply:
  - Point-to-point (during transport)?
  - Endpoint-to-endpoint (during SOAP messaging)?
  - End-to-end (in the payload)?
- What models of authentication, trust, access control, and assertion lookup match your vision?
  - Which existing standard profiles and templates can be leveraged to achieve these?
  - Which expectations need to be adjusted to current reality?
- How to securely manage XBRL documents and associated meta data in a federated environment

First steps on the path to XBRL security nirvana: some software you can play with

- Java Web Services Developer Pack: http://java.sun.com/webservices
- Open-source SAML implementation: http://www.opensaml.org
- Open-source XACML implementation: http://sunxacml.sourceforge.net
- Open-source ebXML Registry implementation: http://ebxmlrr.sourceforge.net

Some conclusions

- Security and identity go hand in hand
- Identity and web services *should* go hand in hand
- New technologies are well-suited to answering XBRL's requirements, in the abstract
  - For granularity, end-to-end treatment, and preserving security data across domain boundaries
- XBRL-enabling vendors have an opportunity to shape the “trusting XBRL” vision in exciting ways
- XBRL International may benefit from liaison with the Liberty Alliance or the SAML committee for profiling work

Thank you!
Questions?

Farrukh Najmi and Eve Maler
farrukh.najmi@sun.com, eve.maler@sun.com
Sun Microsystems, Inc.