Top Ten Web Services Security Issues

QCon 2007
Security Briefing by Arctec Group
(www.arctecgroup.net)

ARCTEC

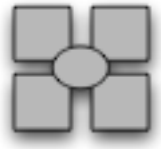
About Arctec Group

- Best in class enterprise architecture consulting provider focused on enterprise, software, and security architecture
- Client list includes numerous global 500 companies, world's largest electronic financial exchanges, emerging startups and Dept. Homeland Security
- Headquarters: IDS Center, Minneapolis, MN; Clientele: global
- Web: www.arctecgroup.net

ARCTEC

About the speaker

- Gunnar Peterson
  - Managing Principal, Arctec Group
  - Editor Build Security In software security column for IEEE Security & Privacy Journal (www.computer.org/security)
  - Primary and contributing author for DHS/CERT Build Security In portal on Web Services security, Identity, and Risk management (https://buildsecurityin.us-cert.gov/daisy/bsi/home.html)
  - Project lead, OWASP XML Security Gateway Evaluation Criteria project (https://www.owasp.org/index.php/Category:OWASP_XML_Security_Gateway_Evaluation_Criteria_Project)
  - Associate editor Information Security Bulletin (www.chi-publishing.com)
  - Contributor Web Application Firewall Evaluation Criteria (http://www.webappsec.org/projects/wafec/)
  - Blog: (http://1raindrop.typepad.com)



Issue 1: You're probably not spending enough money/time/focus on app security

ARCTEC

Cocktail napkin metrics

If I have 100 security dollars where should I spend them?

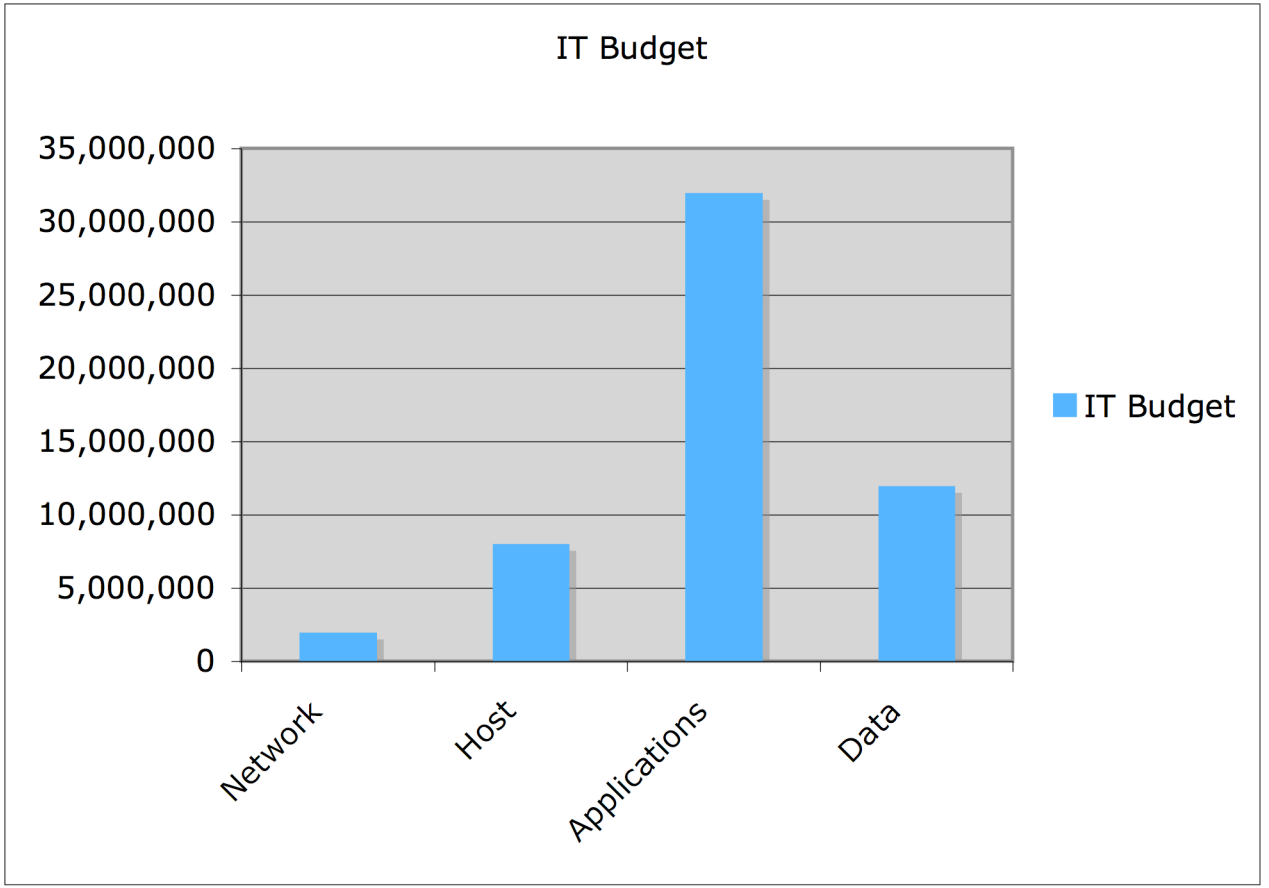
ARCTEC

Investing your $100

- You go to war with the numbers you have not the numbers you wish you had
- Use budget numbers to get at what your business thinks is valuable
- What I learned from Pete Lindstrom - An asset is worth at least what you pay to develop, own, and operate it.
  - Use this to get your floor

ARCTEC

Investing your $100



Where the business spend its money

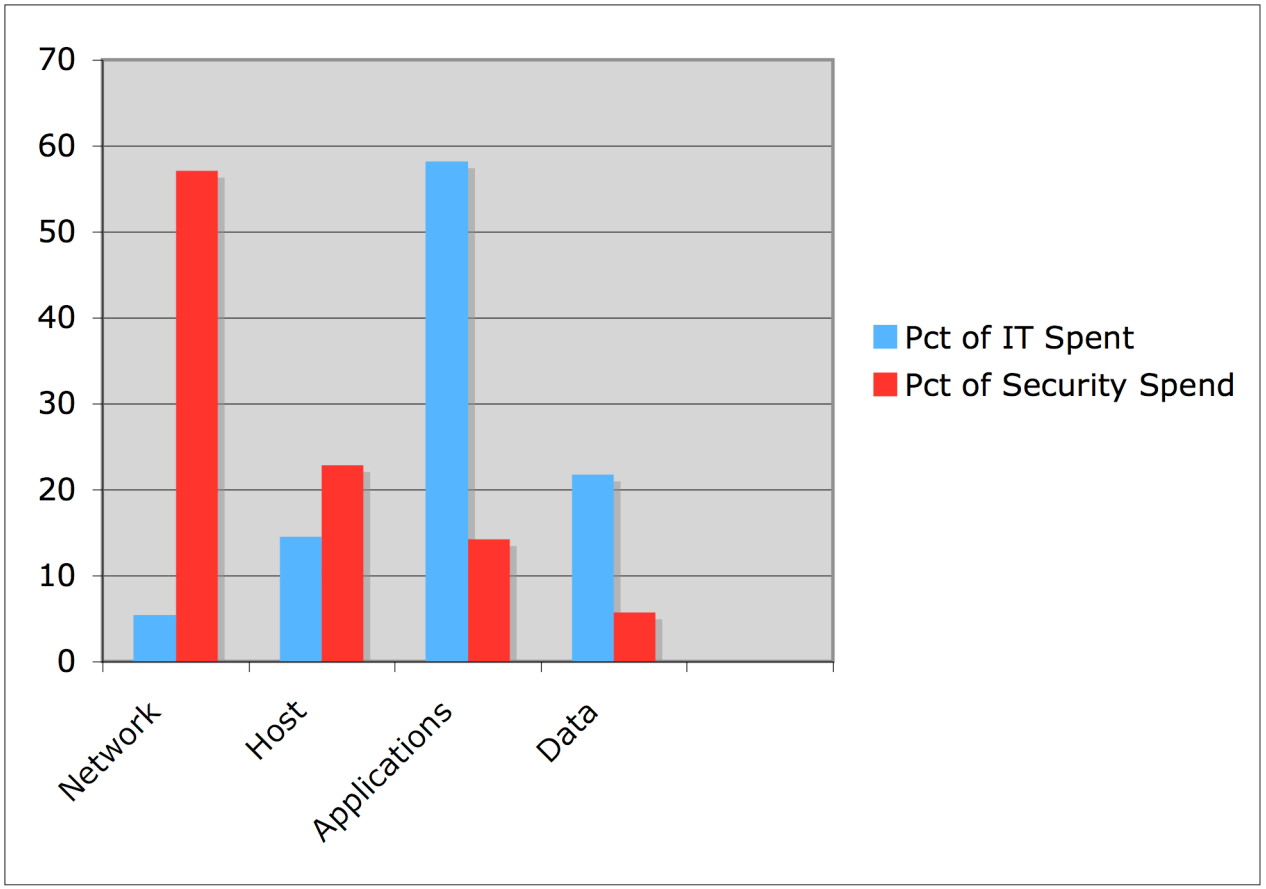
ARCTEC

Investing your $100

	IT Budget	IT Security
Network	2,000,000	750,000
Host	8,000,000	400,000
Applications	32,000,000	250,000
Data	12,000,000	100,000

ARCTEC

	IT Budget	IT Security
Network	3,000,000	1,000,000
Host	8,000,000	400,000
Applications	32,000,000	250,000
Data	12,000,000	100,000
	55,000,000	1,750,000



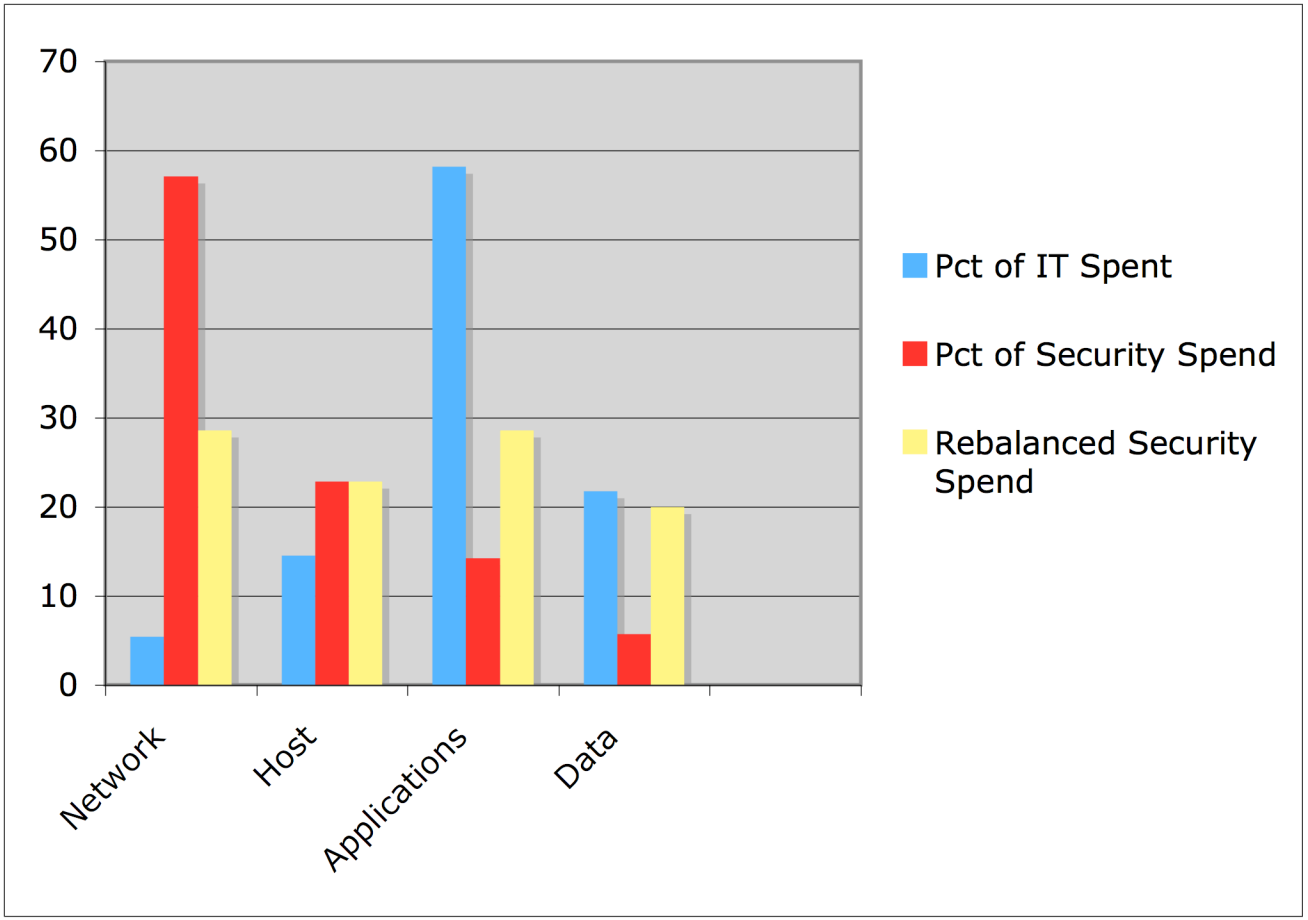
ARCTEC

Reblancing

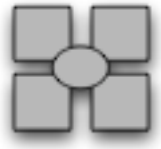
	IT Budget		IT Security
Network	3,000,000		500,000 (-500,000)
Host	8,000,000		400,000 (same)
Applications	32,000,000		500,000 (+250,000)
Data	12,000,000		350,000 (+250,000)
	55,000,000		1,750,000 (same)

ARCTEC

Example - Rebalanced security investment



ARCTEC



Issue 2: Know your security standards

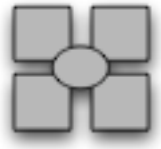
ARCTEC

Security Standards in SOA

Standard	Description
WS-Security	How to attach security tokens to a Web service message
WS-Trust	How to move tokens around in a system
WS-SecureConversation	How to optimize for efficiency
SAML	Authentication, authorization, and attribute assertions
XACML	XML policy language for interoperable security policy

See: DHS Build Security In portal paper by Lipson & Peterson
"**Security Concepts, Challenges, and Design Considerations for Web Services Integration**"
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/assembly/639.html?branch=1&language=1

ARCTEC



Identify standards to address your threats

ARCTEC

STRIDE Threat Model

Threat	Description	SOA Countermeasure
Spoofing	spoofing the identity of a web services requester or provider	?
Tampering	tampering with information, such as the contents of the SOAP body	?
Repudiation	repudiate the receipt or origination of a transaction	?
Information Disclosure	Disclose sensitive information	?
Denial of Service	Disrupt correct operation	?
Elevation of Privilege	attacker gains privileges, such as root	?

More information on STRIDE
http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx

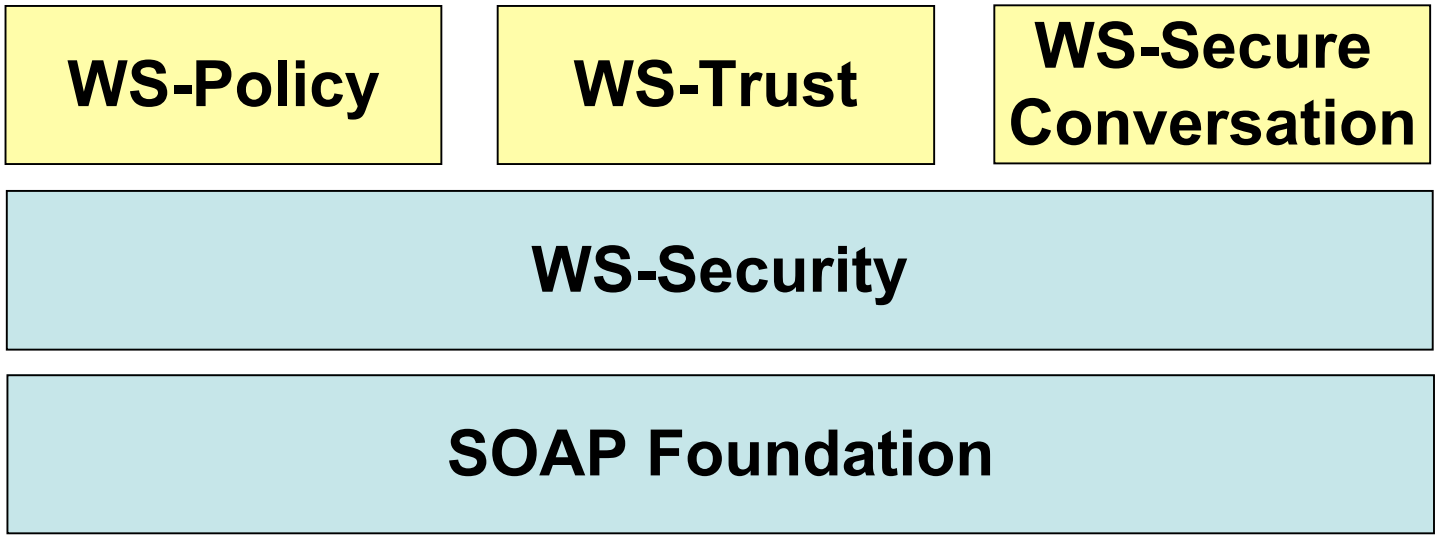
ARCTEC

Hello World SOAP Message

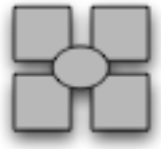
```
<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>

  <getCustomerDetails xmlns="http://servicehost"/>
  <name>Joe Smith</name>
 <customernumber>7301</customernumber>

 </soap:Body>
</soap:Envelope>
```

ARCTEC

Open Security Standards



ARCTEC



Issue 3: Use Message Level Security

ARCTEC

WS-Security

- Requirements (from the spec)
  - Multiple security token formats
  - Multiple trust domains
  - Multiple signature formats
  - Multiple encryption technologies
  - End-to-end message content security and not just transport-level security
- Non-Goals
  - Establishing a security context or authentication mechanisms.
  - Key derivation.
  - Advertisement and exchange of security policy.
  - How trust is established or determined.
  - Non-repudiation.

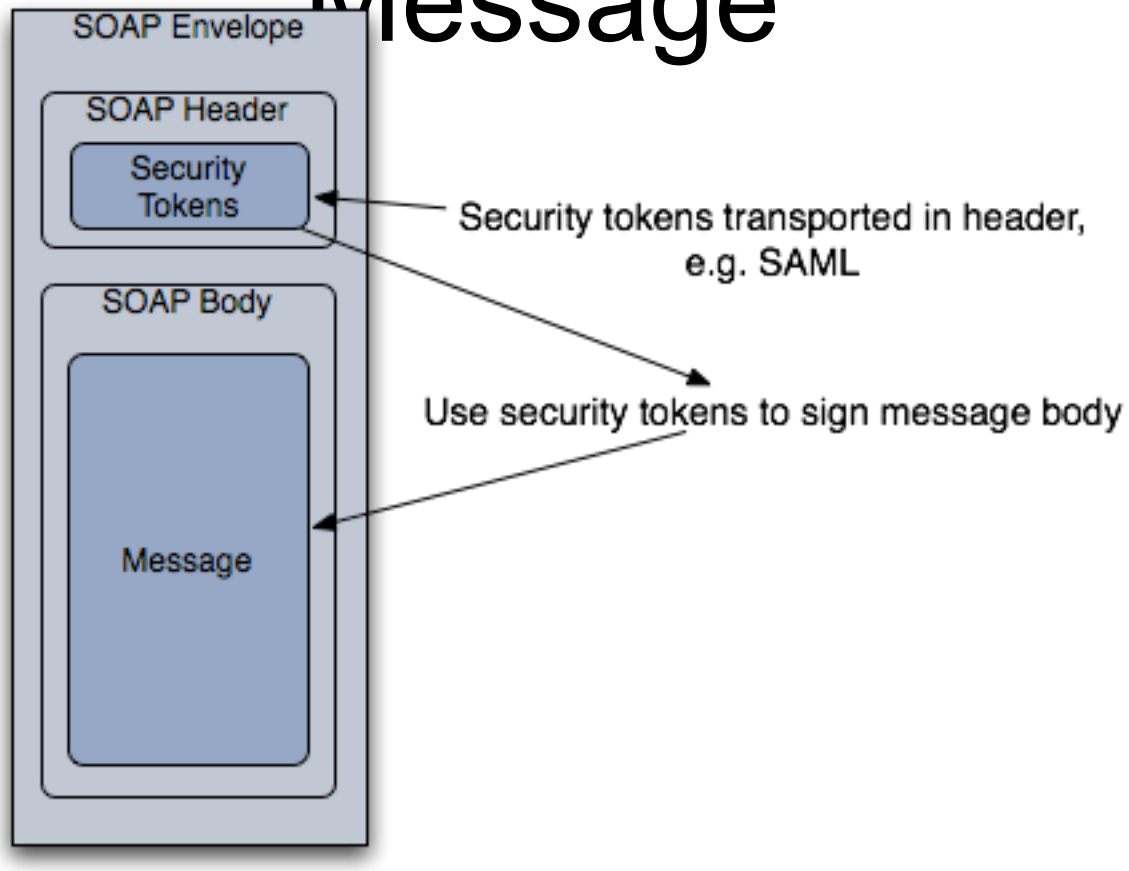
ARCTEC

WS-Security

- SOAP Header for Authentication:
  - Timestamp
  - Multiple Token types identifying principals and keys
    - Unsigned token
      - Username token: username/password
    - Signed token format
      - Kerberos ticket
      - X509: name and public-key
    - XML Token format
      - SAML
  - Signatures (sign message elements with security token's key)
    - XML-DigitalSignature

ARCTEC

Authentication -- Relying on the SOAP Message



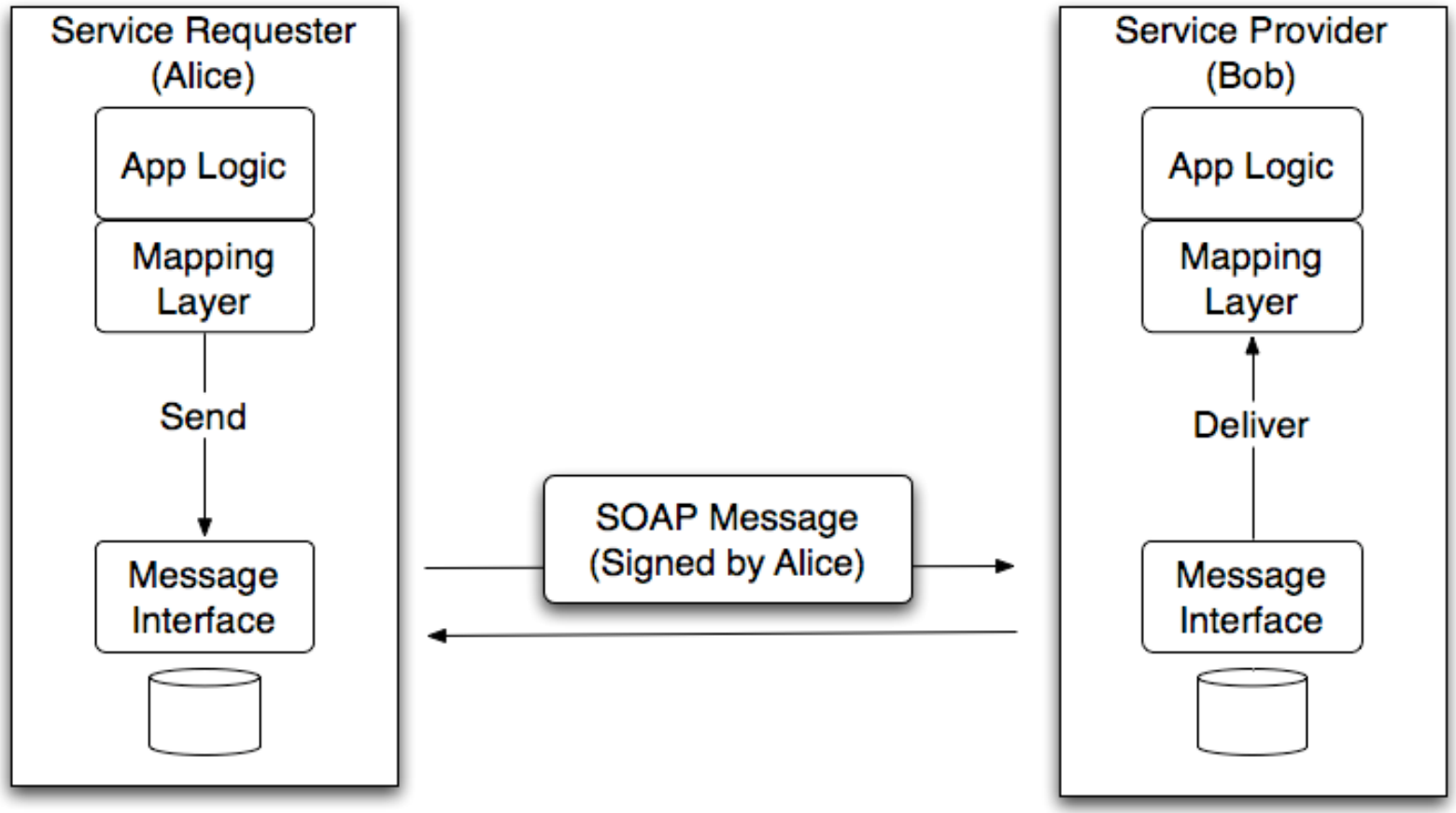
ARCTEC

Hello World SOAP Message

```
<soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>

  <getCustomerDetails xmlns="http://servicehost"/>
  <name>Joe Smith</name>
 <customernumber>7301</customernumber>

 </soap:Body>
</soap:Envelope>
```

ARCTEC

Alice Signs Message

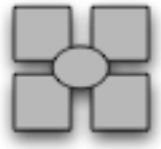


ARCTEC

Hello World + Integrity

```
<soap:Header>
<wsse:Security xmlns:wsse=”…”>
    <dsig:Signature xmlns:dsig=”…Id="Id-00000112eef195a8-…">
<dsig:SignatureValue>…
      <dsig:KeyInfo Id="Id-00000112eef195a8-0000000000000008">
        <dsig:X509Data>
          <dsig:X509Certificate>
            MIICRDCCAaOCBEX67+…
        <dsig:SignatureProperties Id="Id-00000112eef195a8-000a”..>
          <dsig:SignatureProperty Id="Id-00000112eef195a8-09”..
               Target="#Id-00000112eef195a8-0000000000000007">
            <wsu:Timestamp xmlns:wsu=”…”
               wsu:Id="Id-00000112eef195a8-000000000000000b">
              <wsu:Created>2007-06-03T00:17:29Z</wsu:Created>
</wsse:Security></soap:Header>
 <soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
<name>Joe Smith</name>
<customernumber>7301</customernumber>…
```

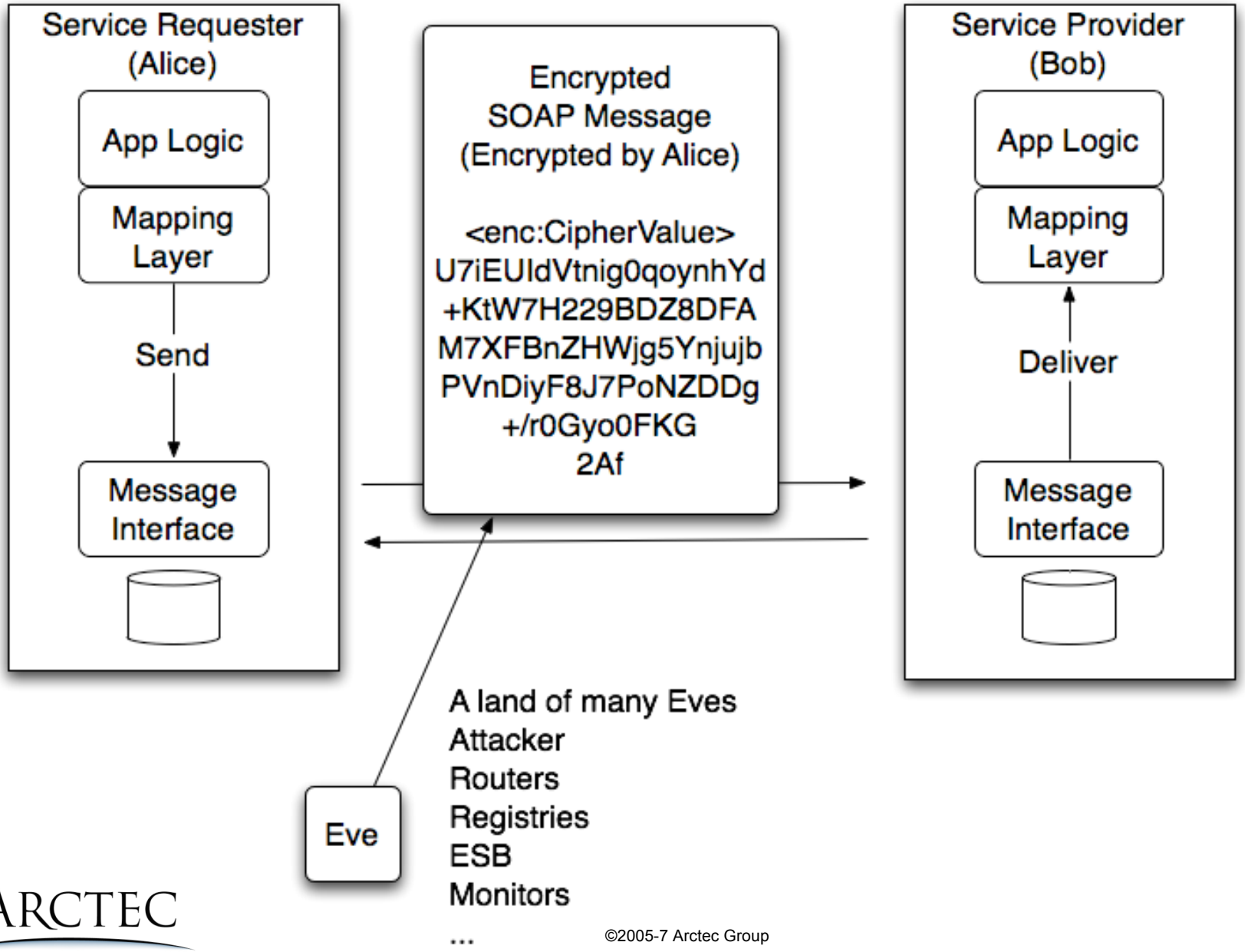
ARCTEC



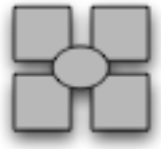
XML Encryption

- Security improvement over the point to point SSL solution
- Encryption may be performed at element level or or all of the document content
- Supports symmetric and asymmetric encryption
- Deals with multi-hop transactions
- Supports granular security models through element level encryption

ARCTEC



ARCTEC



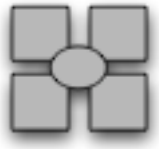
Issue 4: Use Longer Keys

ARCTEC

```
<enc:EncryptionMethod Algorithm=
"http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
```

- 128 bit Security level (“Practical Cryptography”, Schneier & Ferguson)
  - To achieve 128 bit security, use 256 bit symmetric keys
  - Hash function examples: SHA-256, SHA-512
  - MAC example: HMAC-SHA-256

ARCTEC



Issue 5: Validate Input & Encode Output

ARCTEC

- XML Messages can contain a number of nasty things…
  - Injection attacks
    - SQL Injection, Xpath Injection, Xquery Injection
  - XML Denial of Service (XDoS)
    - Using XML as an attack vector
    - Jumbo payloads
    - Recursion
  - Virus in SOAP attachments

ARCTEC

- Schema validation based on hardened schemas

```
<xs:simpleType name=“Zipcode">
   <xs:restriction base="xs:string"
     <xs:pattern value=“([0-9]{5})-([0-9]{4}) "/>
   </xs:restriction>
 </xs:simpleType>
```

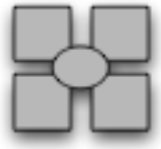
- Semantic validation based on white list or blacklist
  - Regex
- Virus scanning

ARCTEC

Output encoding

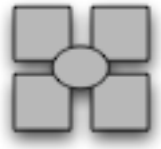
- Don’t propagate attacks

```
<?xml version='1.0'?>
<xsl:stylesheet
xmlns:xsl="http://www.w3.org/1999
/XSL/Transform"
version="1.0">
<xsl:import href=”…docbook.xsl"/>
  <xsl:output method="html"
  encoding="UTF-8"
  indent="no"/>
```



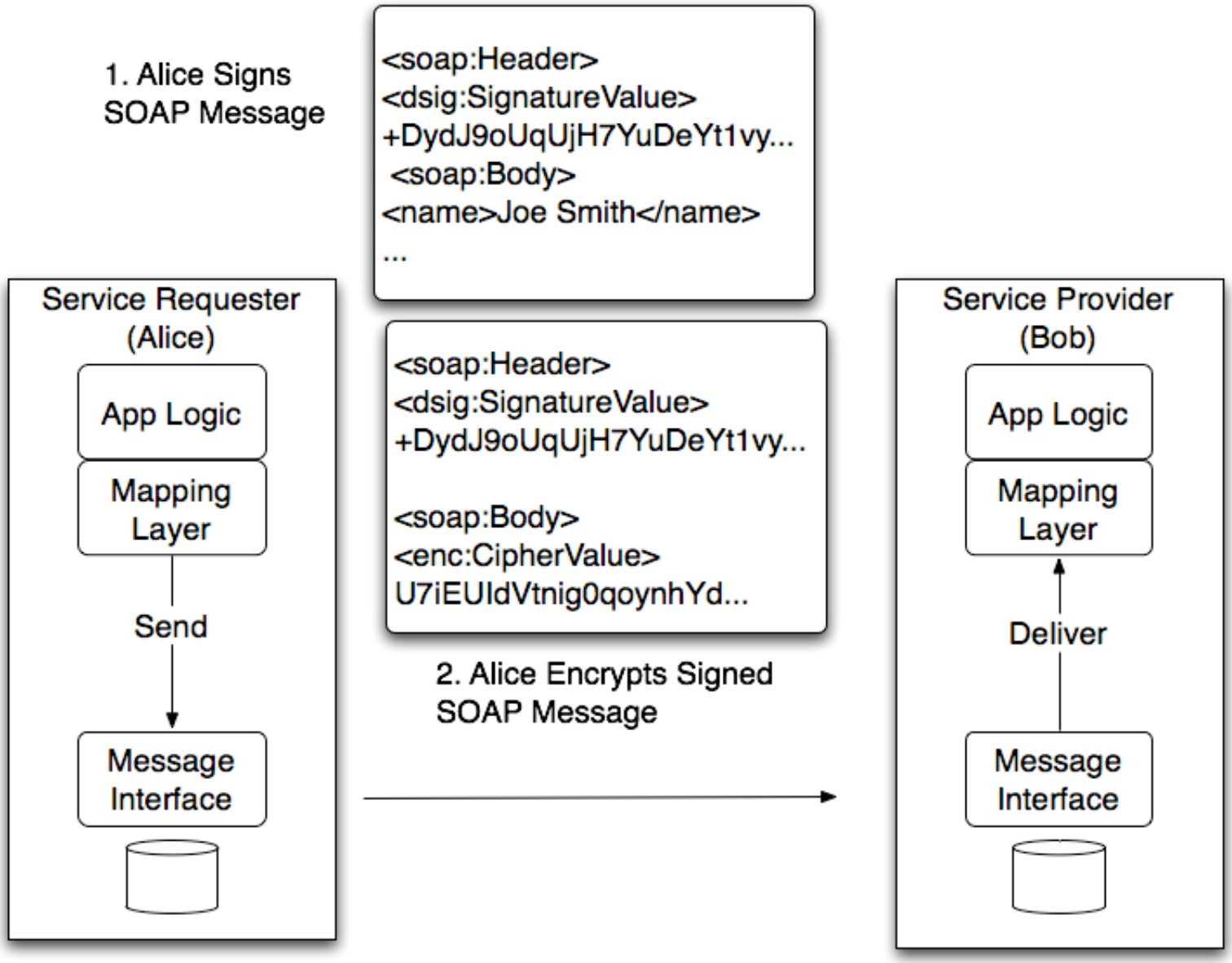
Issue 6: Avoid Naïve Sign & Encrypt

ARCTEC

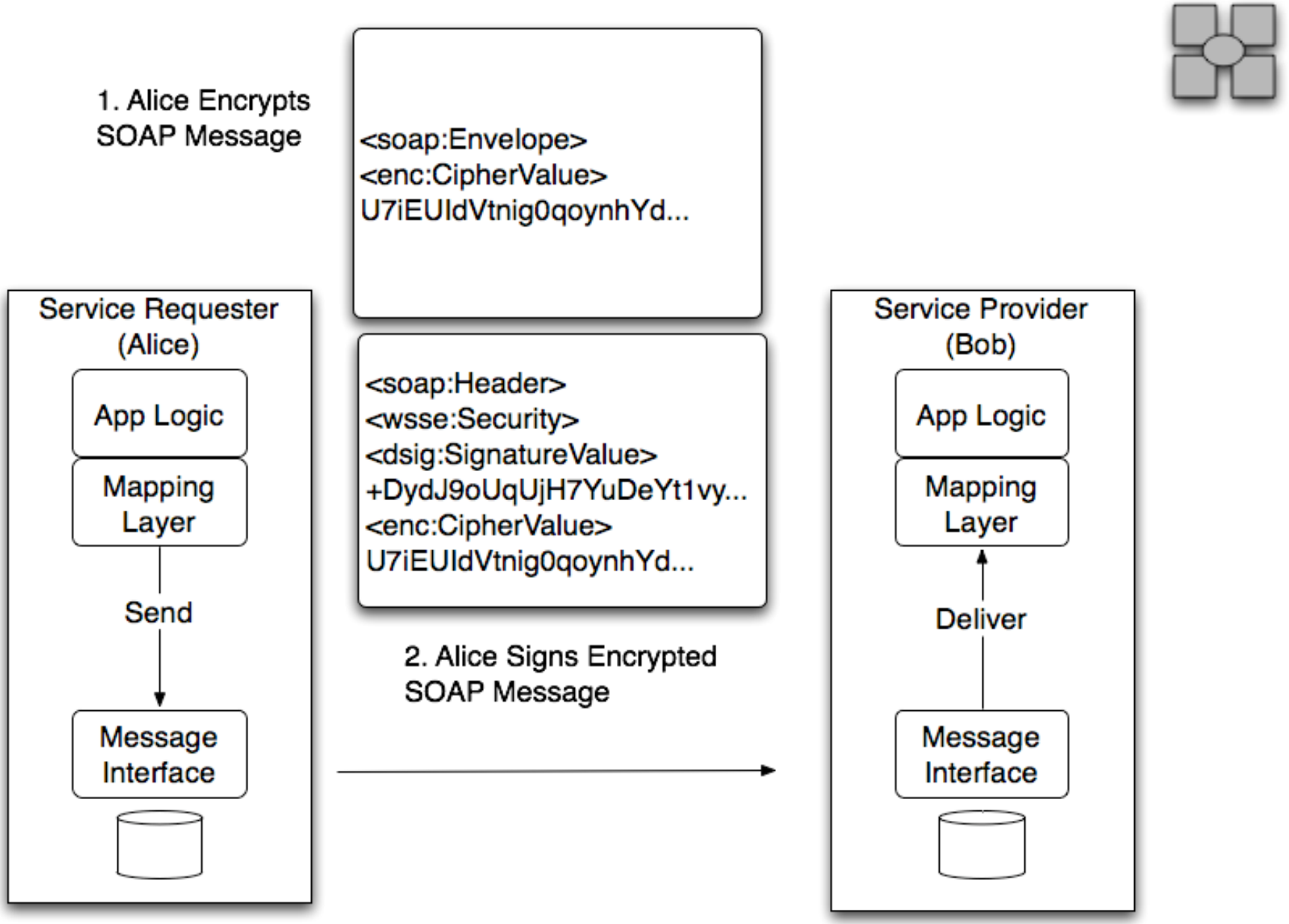


Order of Operations for Sign & Encrypt

ARCTEC



ARCTEC



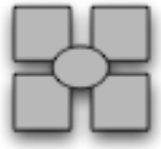
ARCTEC

Design Considerations

Order	Considerations
Sign & Encrypt	-Eve only sees ciphertext - Horton Principle: “Authenticate what you mean not what you say”
Encrypt & Sign	- Theoretic weakness of certain weak encryption schemes - Efficiency gains because Service Provider checks signature first, can discard immediately if message fails authentication

Source: “Practical Cryptography” by Schneier & Ferguson Chapter 8

ARCTEC



But either way there's still a problem…

ARCTEC

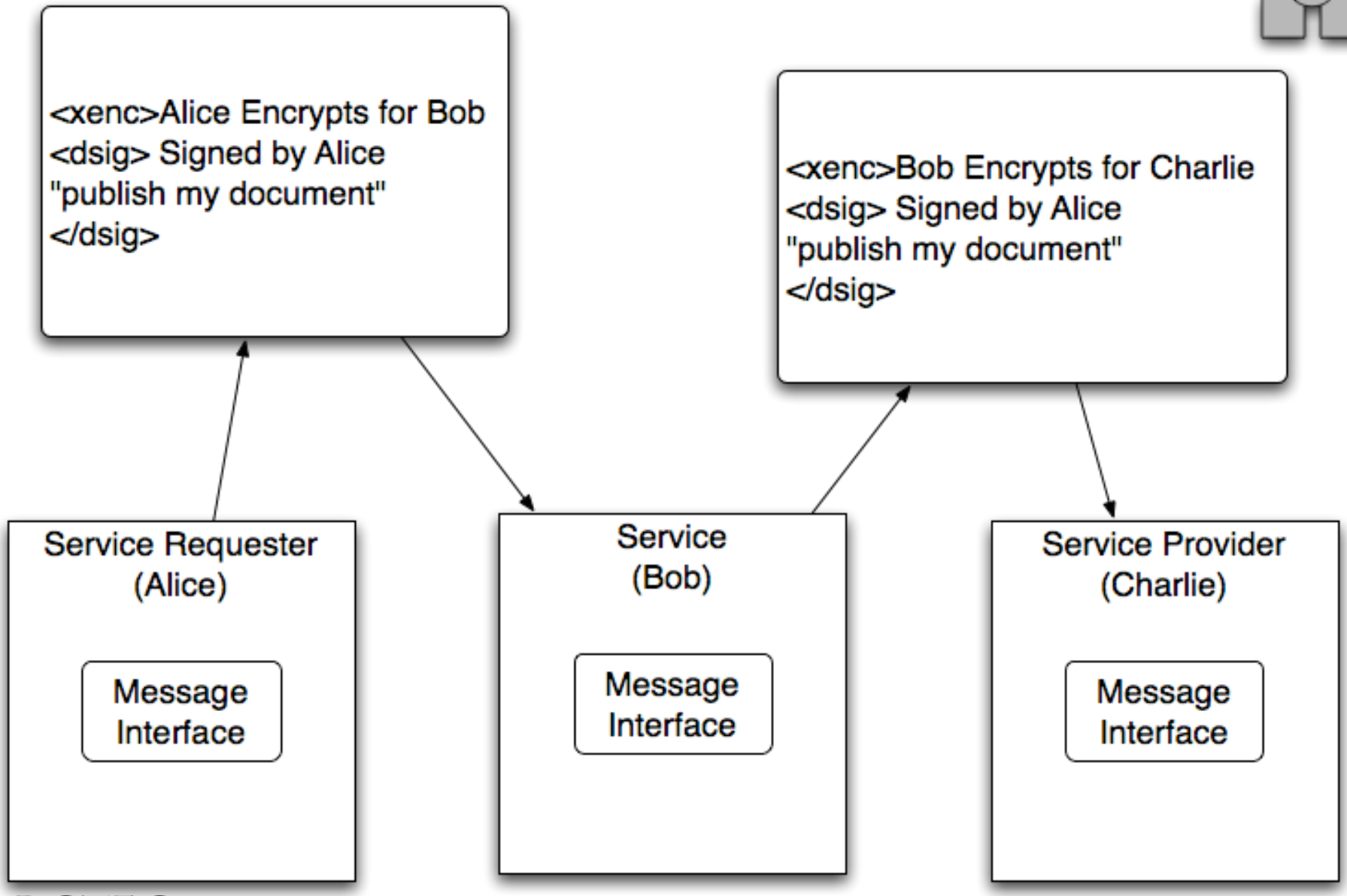
“Defective Sign & Encrypt
S/MIME, PKCS#7, MOSS, PEM, PGP, and XML”

Don Davis

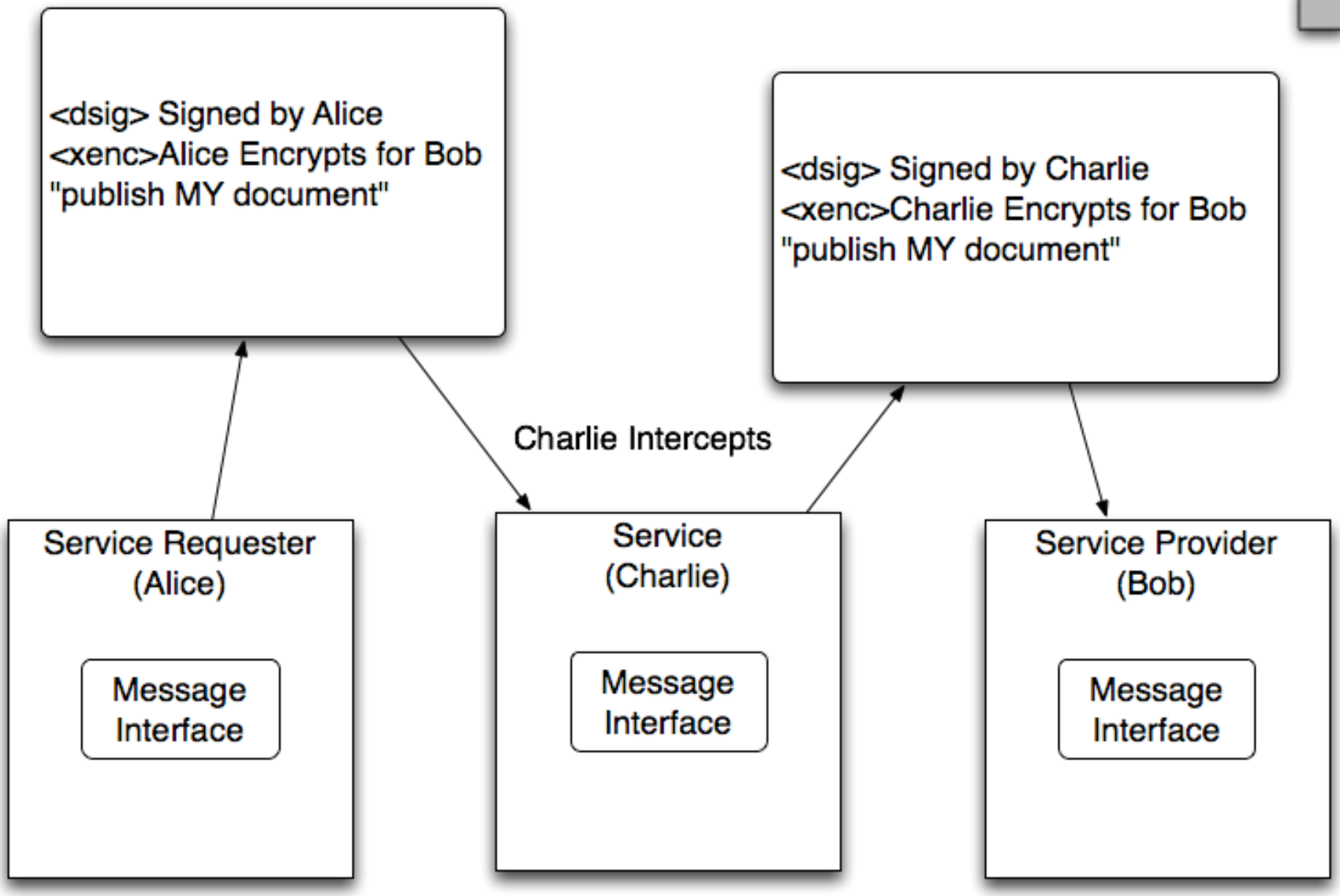
Trust, but verify. - Russian proverb

http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.html

ARCTEC



ARCTEC

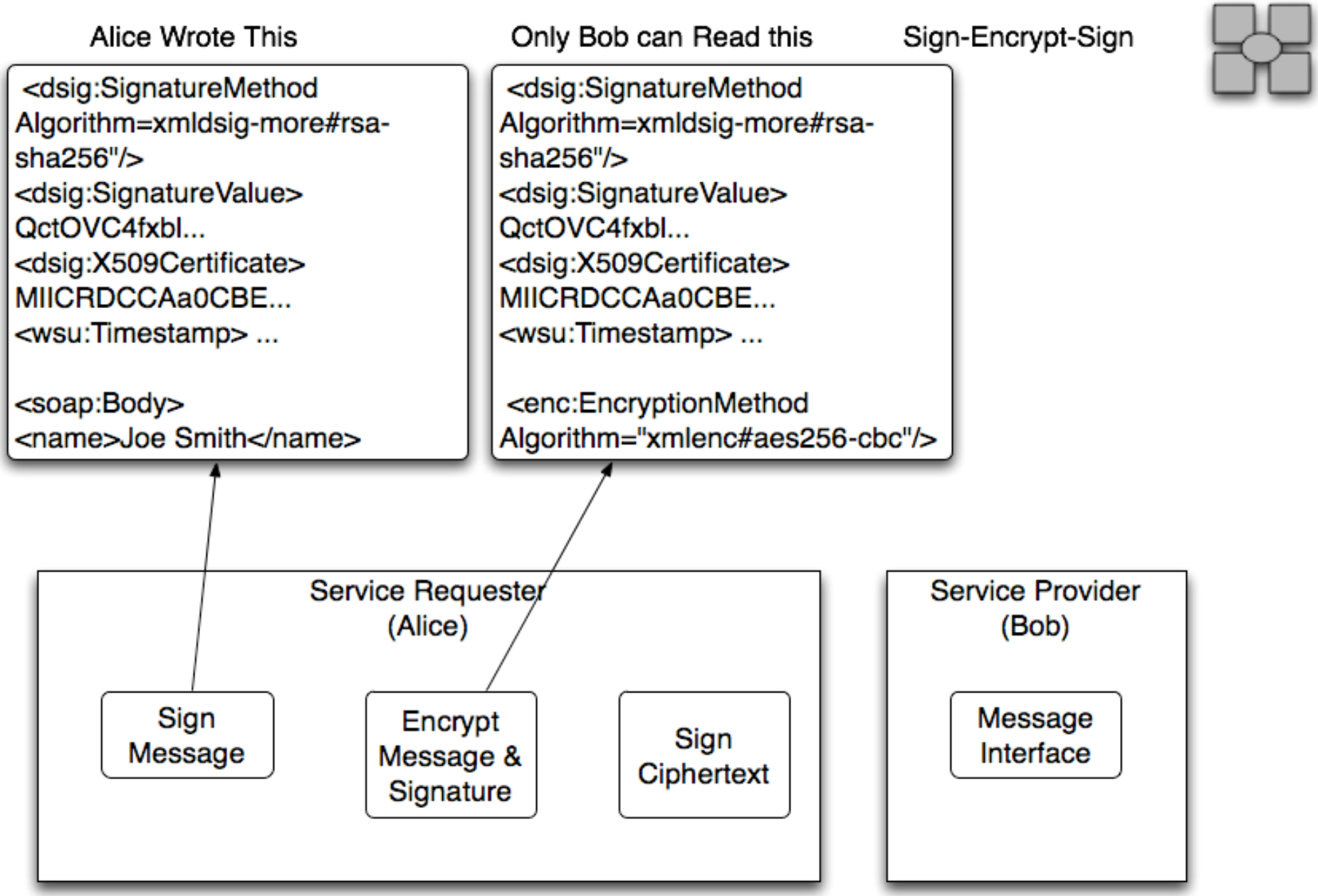


ARCTEC

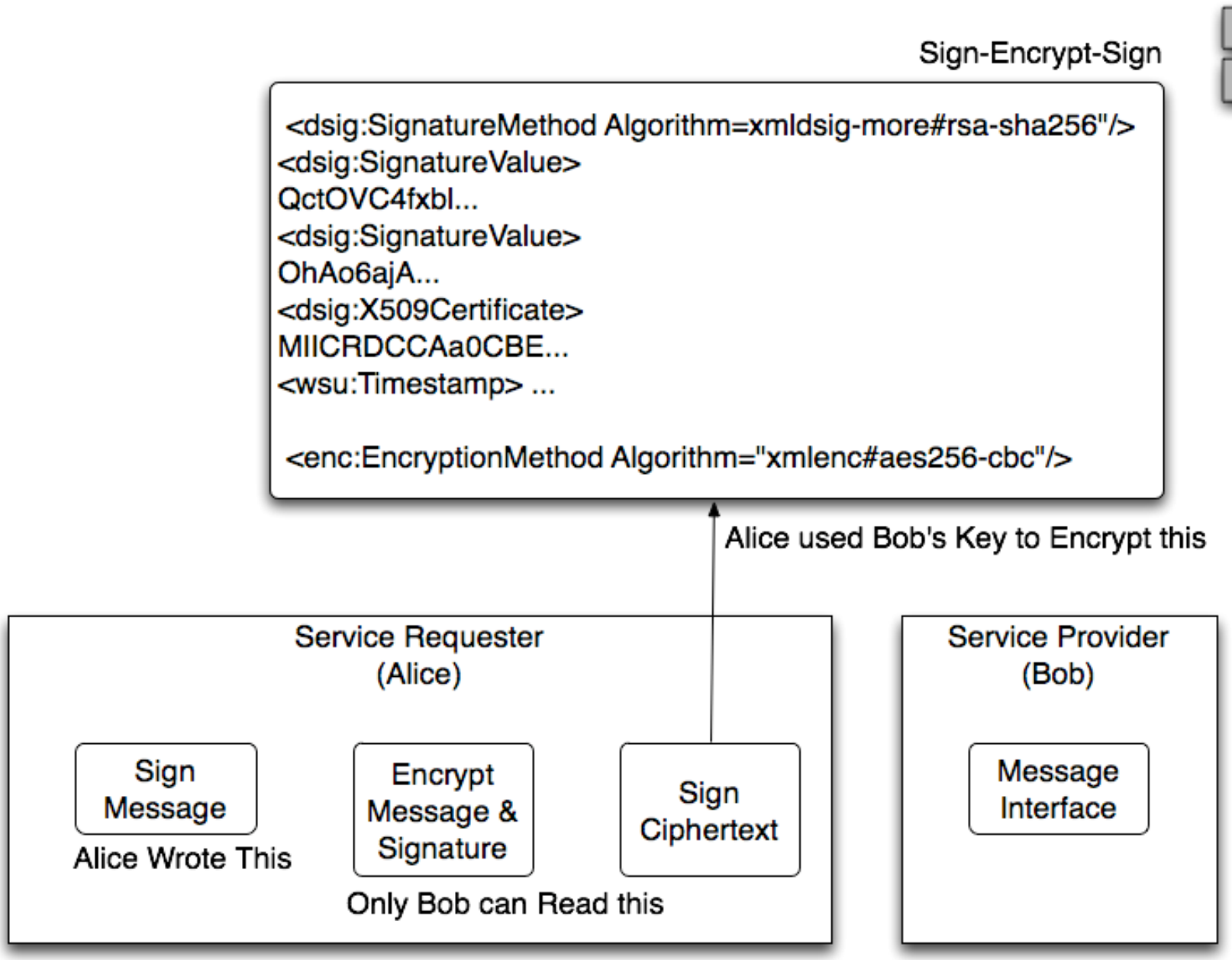
How to fix

1. Sign the recipient's name into the plaintext, or
2. Encrypt the sender's name into the plaintext, or
3. Incorporate both names; or
4. Sign again the signed-&-encrypted message; or
5. Encrypt again the signed ciphertext.

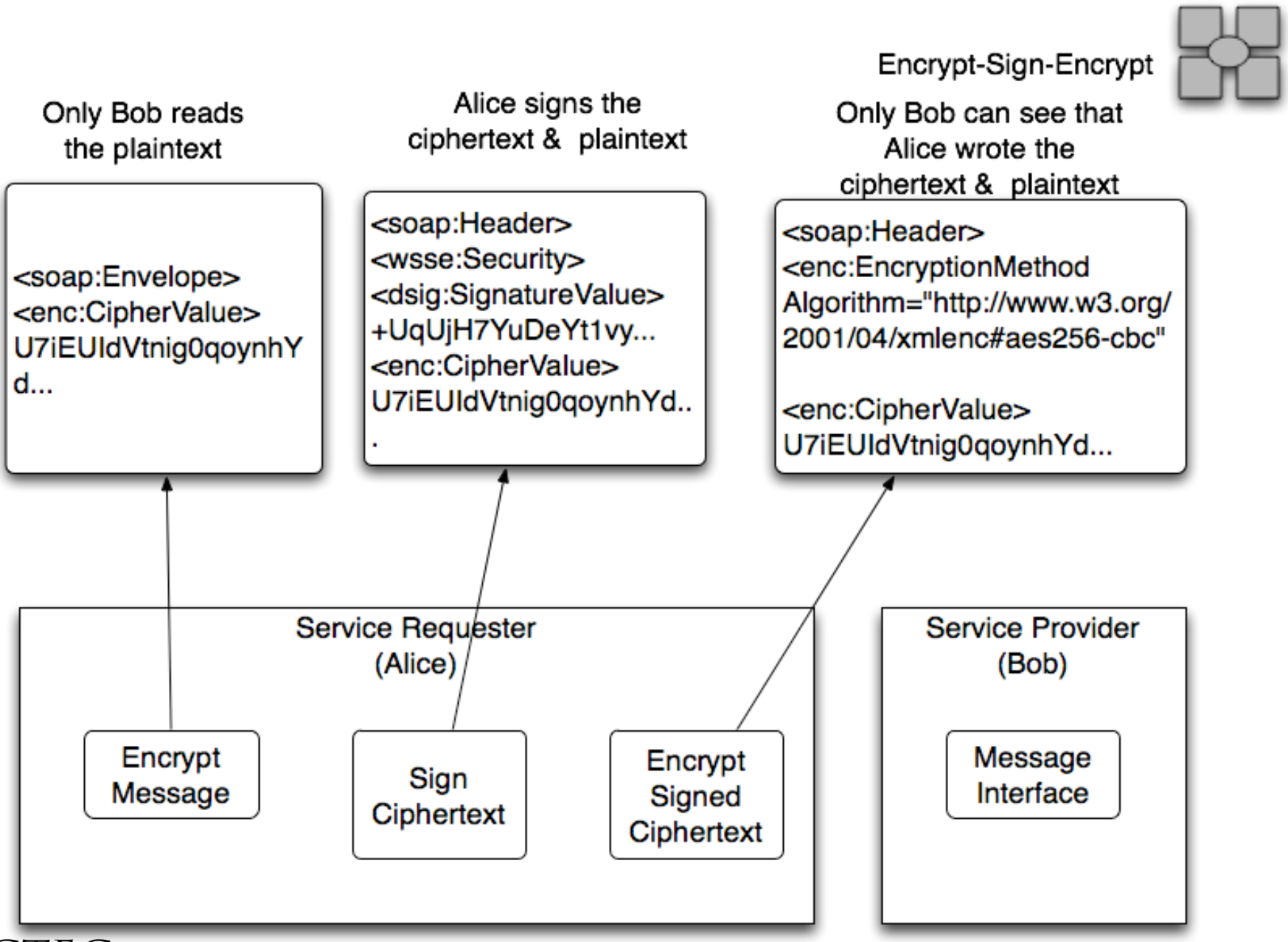
ARCTEC



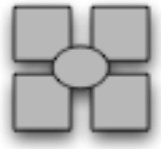
ARCTEC



ARCTEC



ARCTEC

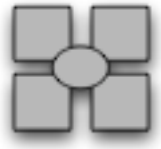


Issue 7: Scan Your Stuff Before Someone Else Does

ARCTEC

Web Services Vuln Assessment

- Test covert channels
  - CData tunneling
  - Inject commands/data into XML request
- Test for XDoS
- Test correct operations in unexpected order
- Test request and response
- Send attachments
- Scan for directories containing files, extensions that allow attacker to footprint system
- Scan host for any other services
- Vulnerability assessment tools
  - iSec http://www.isecpartners.com/tools.html
  - NetSquare http://net-square.com/ns_freetools.shtml
  - OWASP - WebScarab (www.owasp.org)



Issue 8: XDoS

ARCTEC

DTD Recursion Attack

```
<!DOCTYPE foobar [
<!ENTITY x0 "hello">
<!ENTITY x1 "&x0;&x0;">
<!ENTITY x2 "&x1;&x1;">
<!ENTITY x3 "&x2;&x2;">
<!ENTITY x4 "&x3;&x3;">
...
<!ENTITY x98 "&x97;&x97;">
<!ENTITY x99 "&x98;&x98;">
<!ENTITY x100 "&x99;&x99;">     ]>
 <foobar>&x100;</foobar>
```

Source Vordel Taxonomoy of XML Attacks

ARCTEC

XDoS

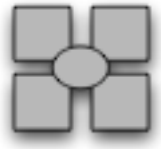
- Attacker sends XML bomb(s) to service
  - Can be used to attack CPU through recursion
  - Can attack memory by targeting DOM to create very large trees in memory
  - Can attack network with numerous small files

ARCTEC

XDoS in the SOAP header

```
<SOAP>
  <Header>
    <wsse:Security>
      1 GB Binary blob
     <Signature>…</Signature>
    </wsse:Security>

  </Header>
  <Body>
    <GetCustomerData>
    </Account>1234</Account>
    </GetCustomerData>
  </Body>
</SOAP
```

ARCTEC

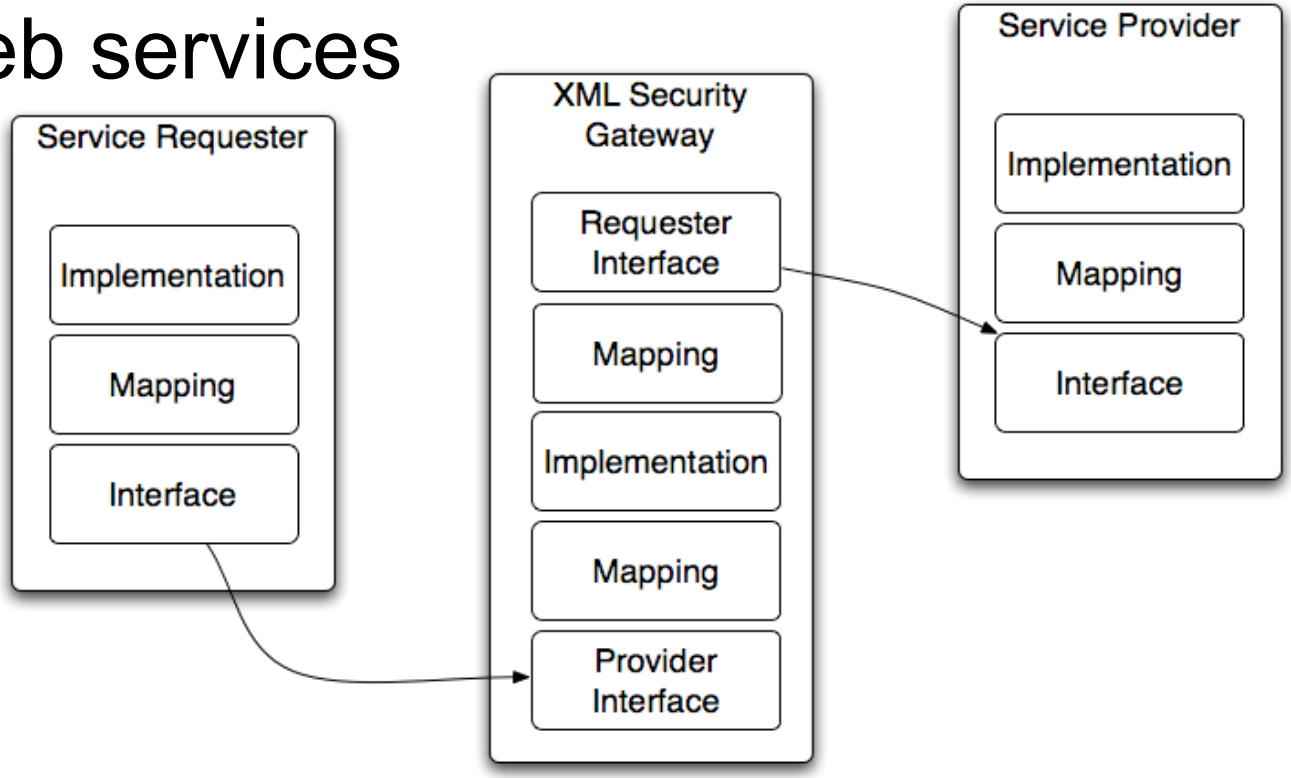


Issue 9: Implement a XML Security Gateway

ARCTEC

- Context: The primary goal of Web services is to solve interoperability and integration problems. Web services traverse multiple technologies and runtimes.
- Problem: Web service requesters and providers do not agree upon binary runtimes like J2EE, instead they agree upon service contracts, message exchange patterns, and schema. Service and message level authentication, authorization, and auditing services for Web services are not delivered by a single container, rather these services must span technical and organizational boundaries

- Solution: Use a XML Security Gateway to provide decentralized security services for Web services



ARCTEC

```
<wsse:Security xmlns:wsse="http://schemas.xmlsoap.org/ws/2003/06/secext">
    <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
AssertionID="Id-000001129354af1c-0000000000000002" IssueInstant="2007-05-
16T05:20:39Z" Issuer="CN=Test,OU=Unknown" MajorVersion="1" MinorVersion="1">
      <saml:Conditions NotBefore="2007-05-16T04:40:35Z" NotOnOrAfter="2007-05-
16T06:40:35Z"/>
      <saml:AuthorizationDecisionStatement Decision="Permit"
Resource="http://host/service">
        <saml:Subject>
          <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">Test</saml:NameIdentifier>
        </saml:Subject>
        <saml:Action>getCustomerDetails</saml:Action>
      </saml:AuthorizationDecisionStatement>
<dsig:SignatureValue>V6pRhOSnrvS8xT+WXIbNvlrOhVkAUMVI4YZ27KfG/jDLMwSbrsD6E3tA4
OrI6naL
U+gt2OsYr58rD+AILpxNk0uxZMWdLcj3zr0gljt339DvYL6MRJBZ3KvpDmrw16PM
w8Wo7ac1tGcLFVW5PV5locPs+f0V+rOGHafYTGGlubQ=</dsig:SignatureValue>
        <dsig:KeyInfo Id="Id-000001129354af1d-0000000000000004">
          …
    </saml:Assertion>
  </wsse:Security>
  </soap:Header>
 <soap:Body>
<ns0:getCustomerDetails xmlns:ns0="http://servicehost"/>
<customernumber>1234</customernumber>
```

Choosing a XSG

- OWASP XML Security Gateway Evaluation Criteria Project
  - * Create evaluation criteria supporting a transparent, level playing field for XML Security Gateway solutions to define their solution's key value proposition
  - * Where practical, attempt to standardize nomenclature and metrics
  - * Educate the community on the design considerations for XML security

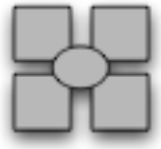
ARCTEC

Choosing a XSG (cont.)

- OWASP XML Security Gateway Evaluation Criteria Project
  - Section 1 - Authentication
  - Section 2 - Authorization
  - Section 3 - Audit Logging
  - Section 4 - Deployment Architecture
  - Section 5 - Content Validation
  - Section 6 - Management & Metrics
  - Section 7 - Transformation
  - Section 8 - Tools

Threat	Description	Countermeasure
Spoofing	spoofing the identity of a web services requester or provider	XML-Sig
Tampering	tampering with information, such as the contents of the SOAP body	XML-Sig
Repudiation	repudiate the receipt or origination of a transaction	XML-Sig
Information Disclosure	Disclose sensitive information	XML-Enc
Denial of Service	Disrupt correct operation	XSG
Elevation of Privilege	attacker gains privileges, such as root	XSG, Input validation

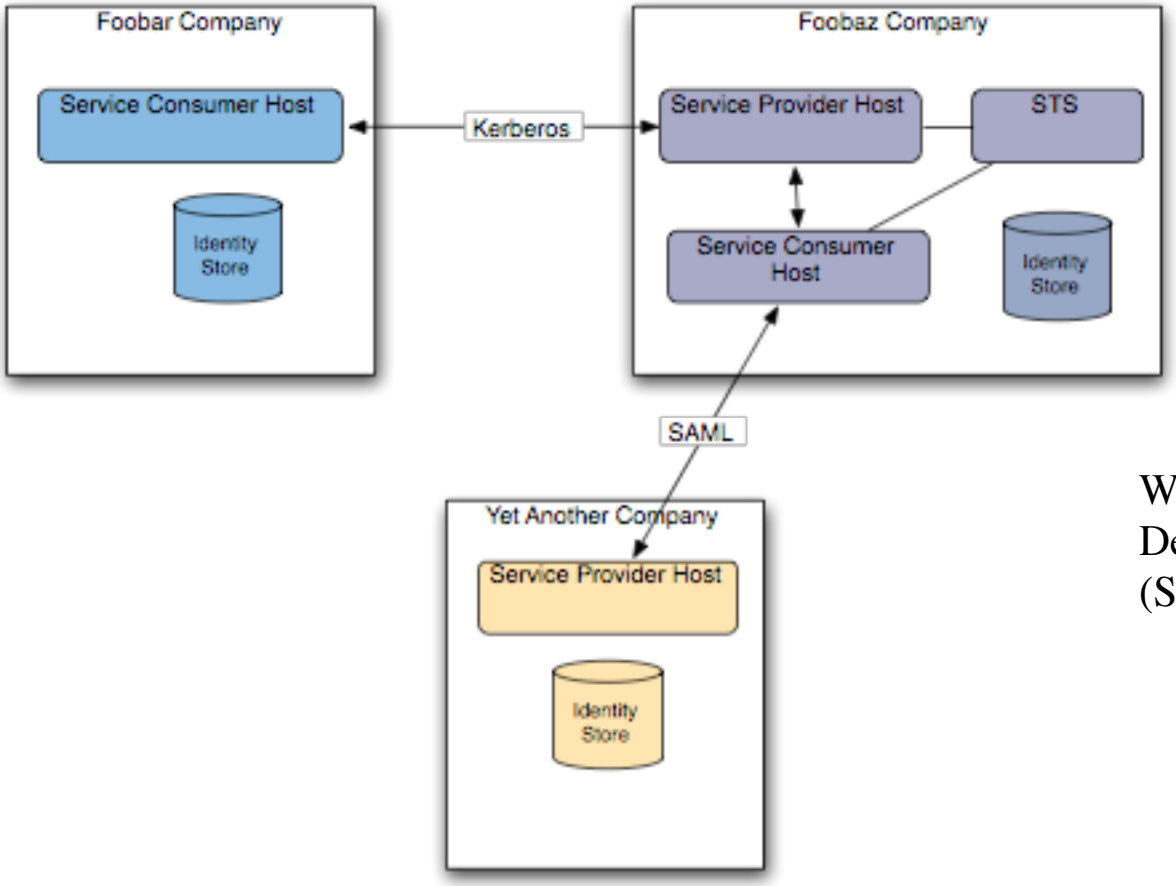
ARCTEC



Issue 10: Identity Enablement in Web Services

ARCTEC

WS-Trust: Beyond Point to Point

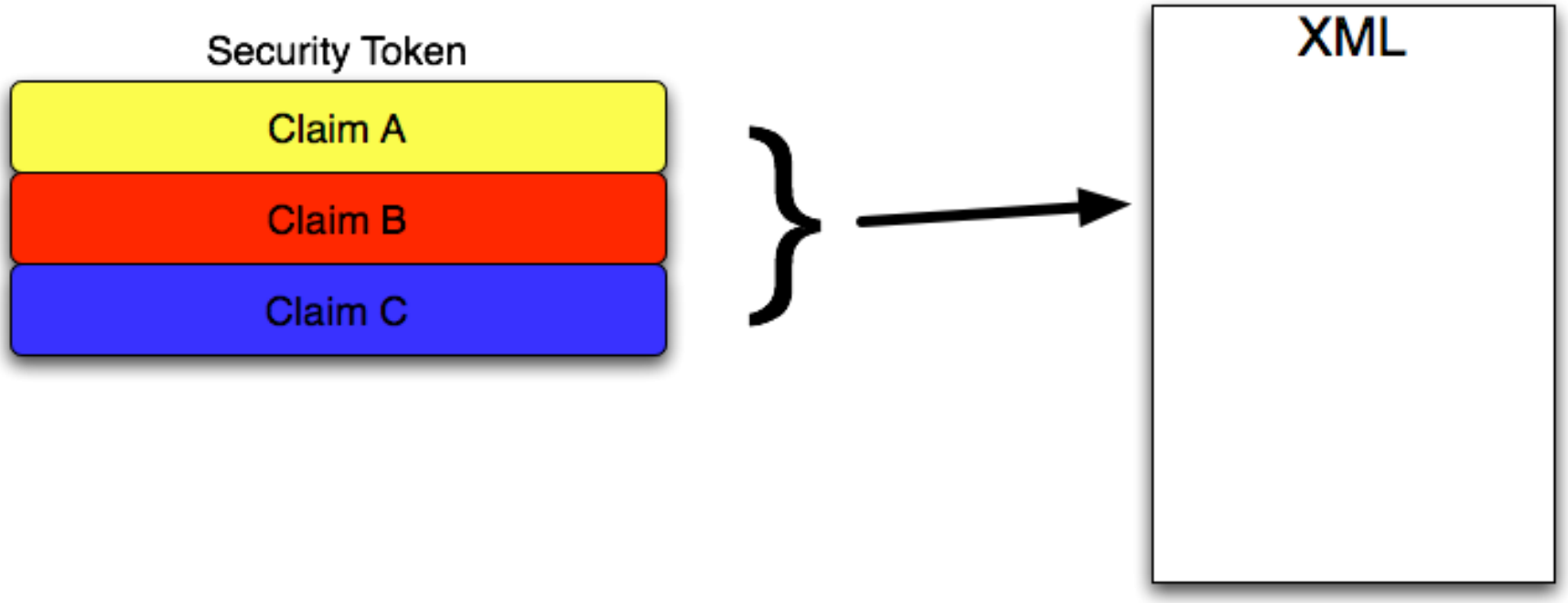


WS-Trust
Defines a Security Token Server (STS)

- Create security tokens
- Validate security tokens

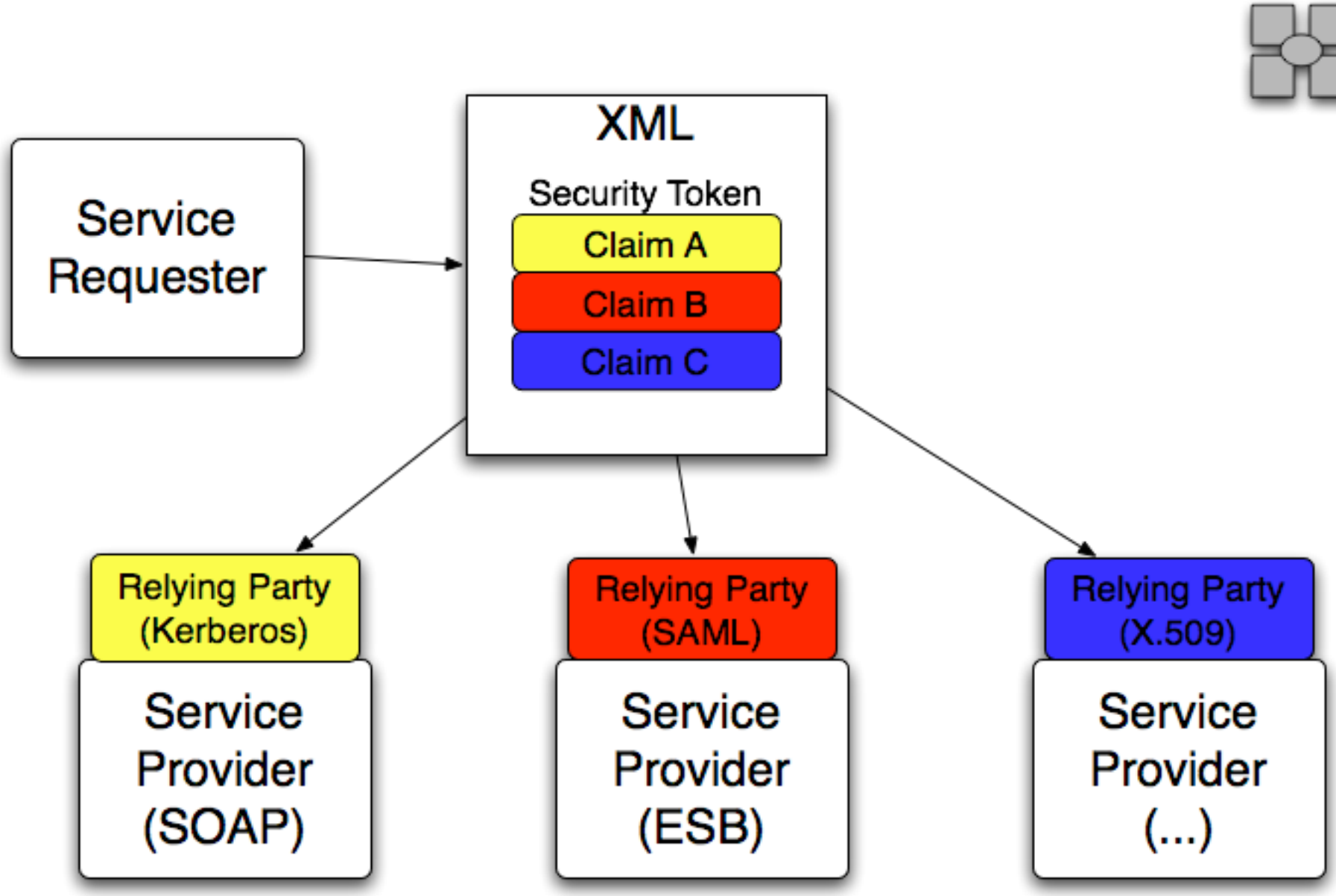
ARCTEC

Claims

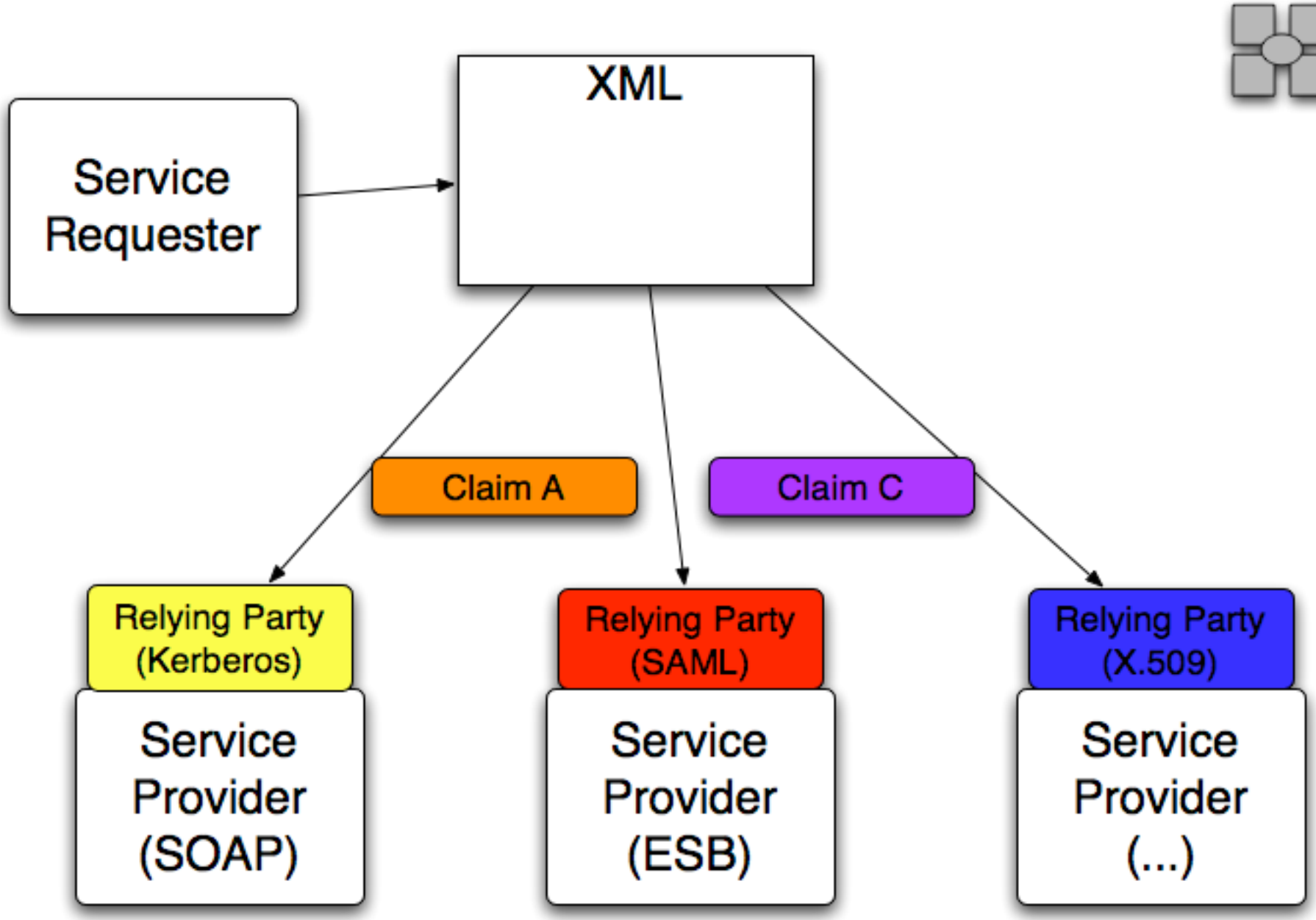


OED - “An assertion of the truth of something, typically one which is disputed or in doubt.”

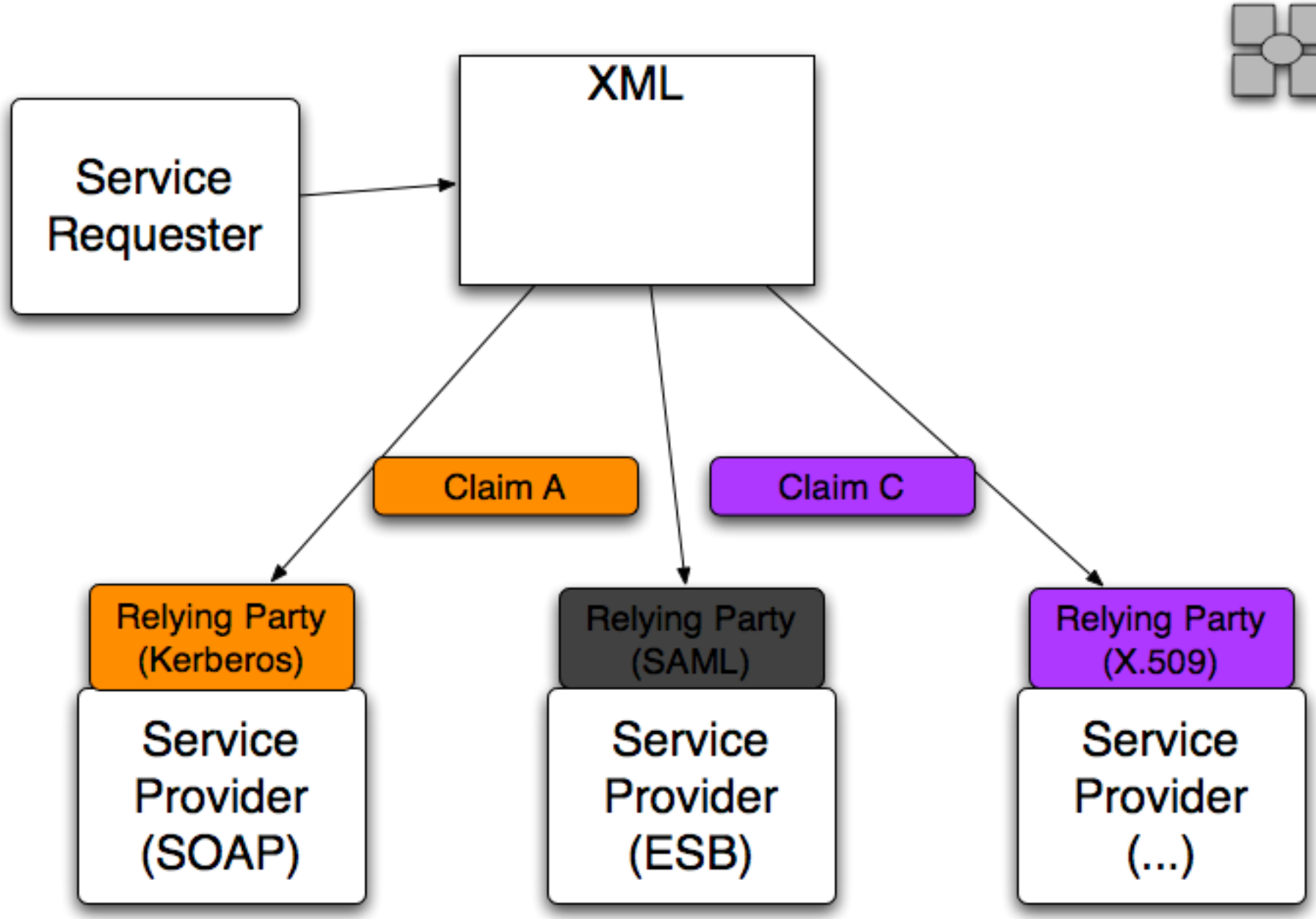
ARCTEC



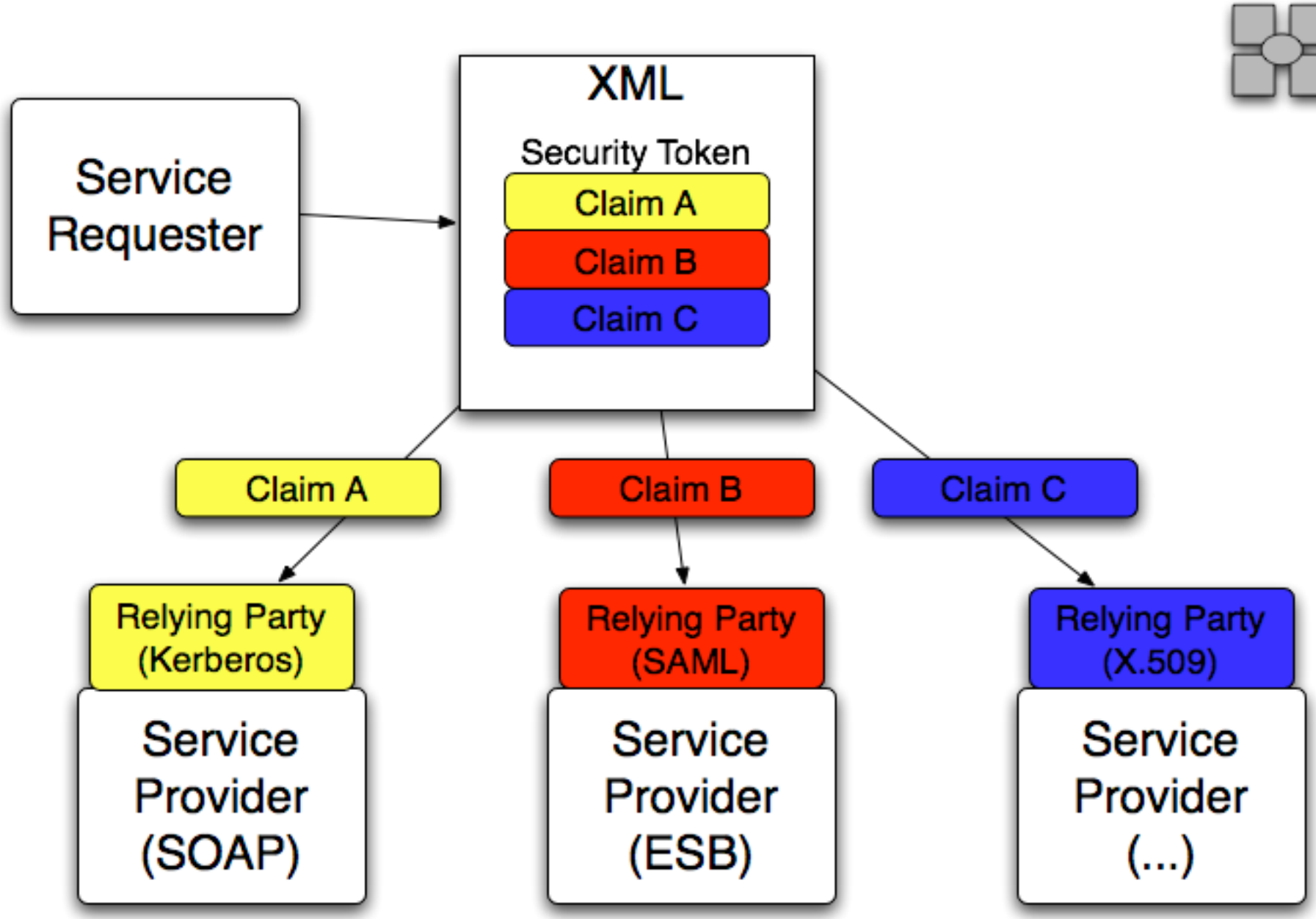
ARCTEC



ARCTEC

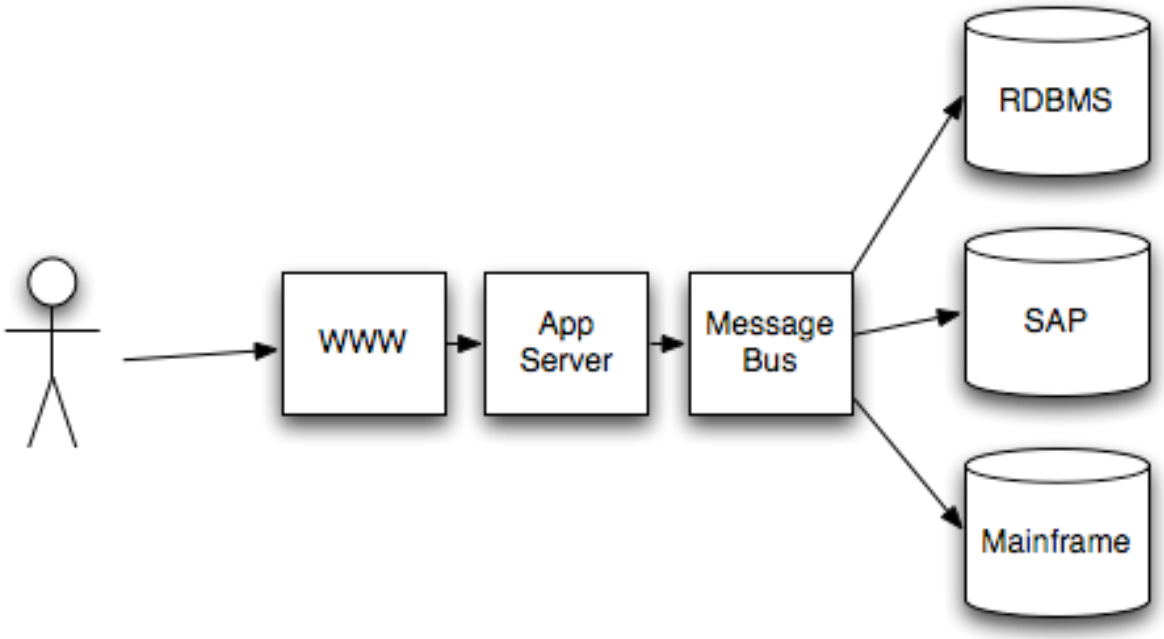


ARCTEC



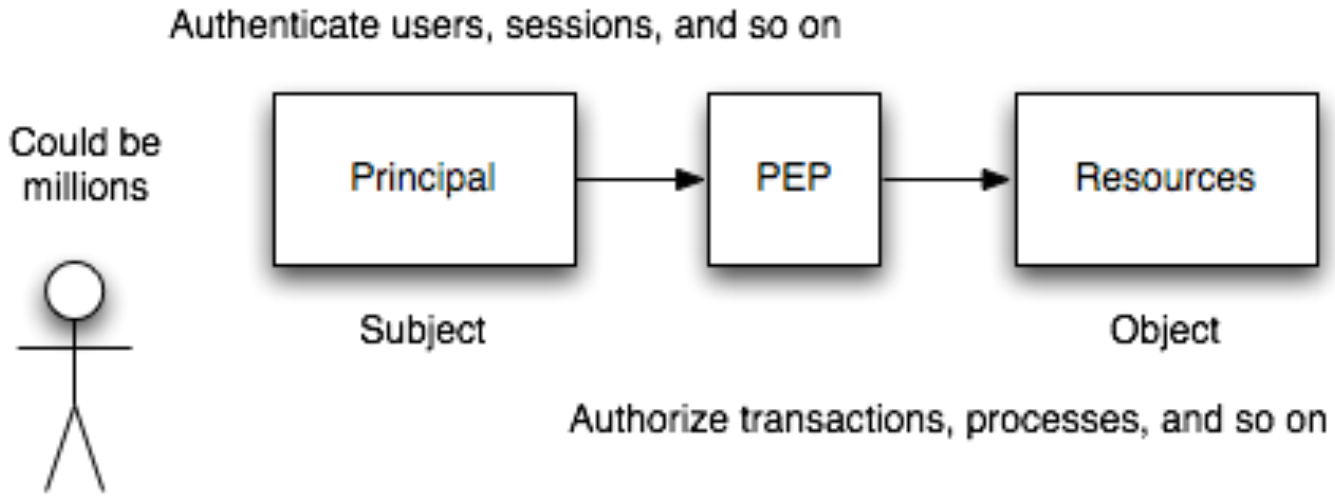
ARCTEC

Design Patterns



ARCTEC

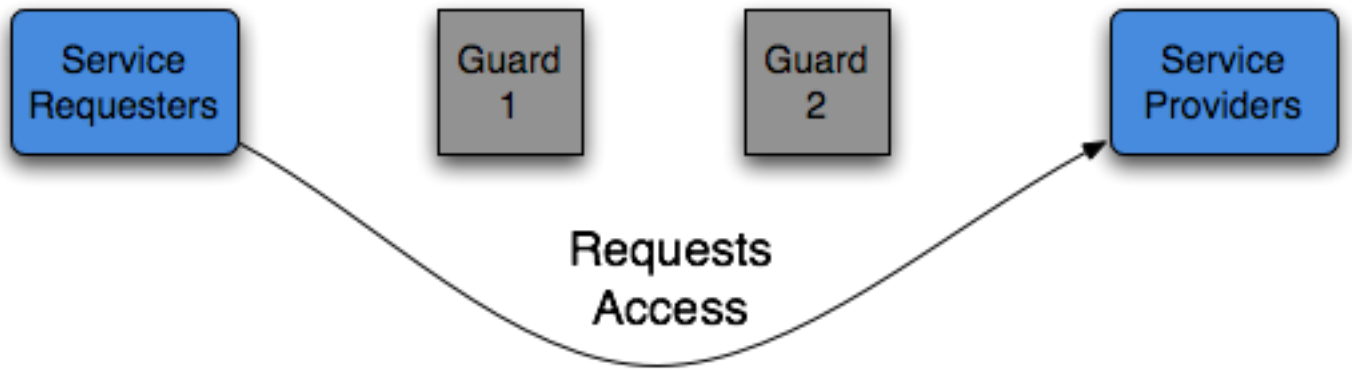
Design Patterns



ARCTEC

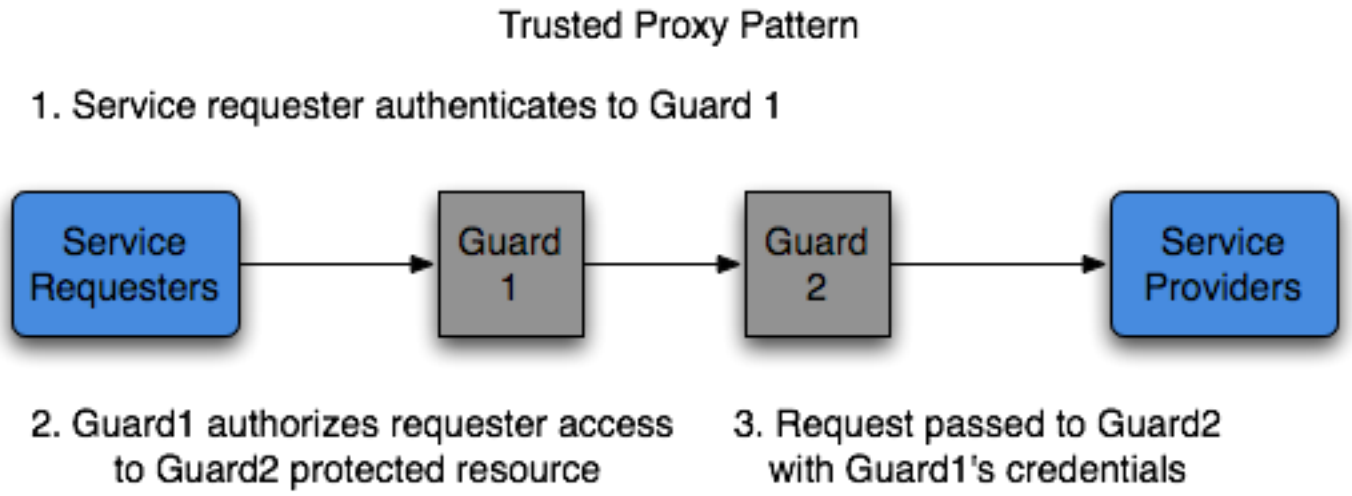
Security Design Patterns

- Secure Proxies Pattern from
  - Blakley & Heath “Security Design Patterns” http://www.opengroup.org/bookstore/catalog/g031.htm



ARCTEC

Example Proxy Pattern

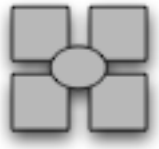


	Passwd to guard1	Userid to guard2	Guard2 authn	Guard2 authz	Sso	Delegation protocol
Ideal	No	Yes	User	User	Yes	No
Trusted proxy	No	*No*	*Guard1*	*Guard1*	Yes	No

Blakley & Heath "Security Design Patterns" http://www.opengroup.org/bookstore/catalog/g031.htm

ARCTEC

Security Design Patterns

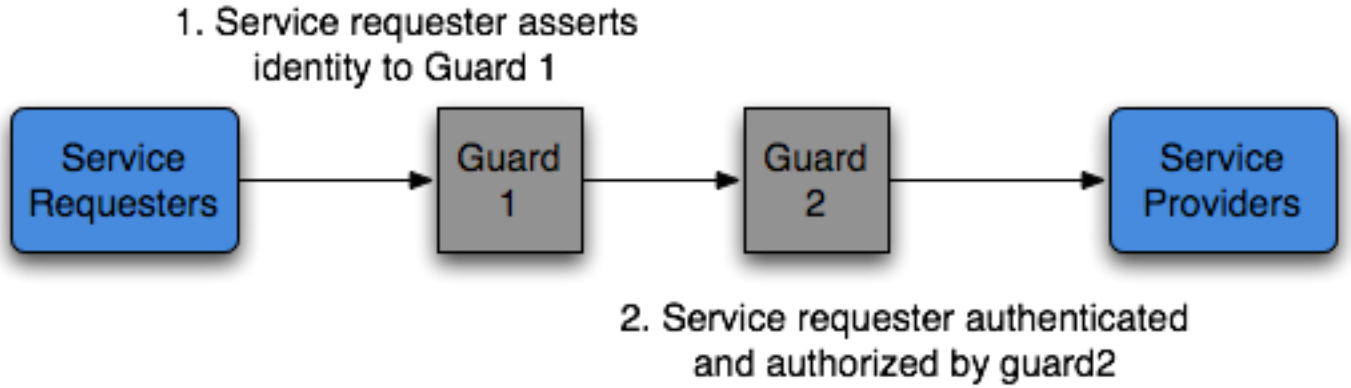


	Passwd to guard1	Userid to guard2	Guard2 authn	Guard2 authz	Sso	Delegation protocol
Ideal	No	Yes	User	User	Yes	No
Trusted proxy	No	*No*	*Guard1*	*Guard1*	Yes	No
Authn impers	*Yes*	Yes	User	User	Yes	No
Id-assert impers	No	Yes	*No*	User	Yes	No
Delegate	No	Yes	User	User	Yes	*Yes*
Authz proxy	No	*No*	*No*	*No*	Yes	No
Login tunnel	No	Yes	User	User	*No*	no

ARCTEC

Blakley & Heath "Security Design Patterns" http://www.opengroup.org/bookstore/catalog/g031.htm

Towards an Ideal Proxy

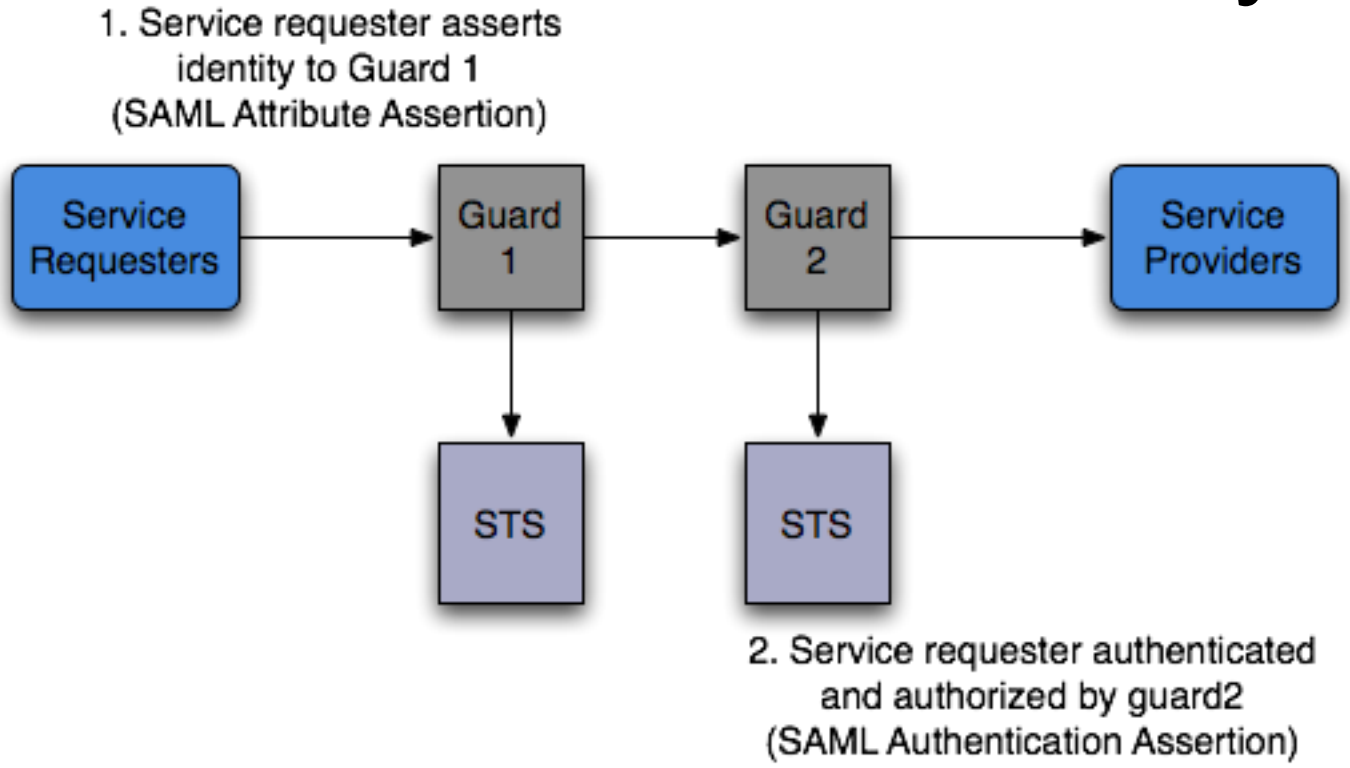


	Passwd to guard1	Userid to guard2	Guard2 authn	Guard2 authz	Sso	Delegation protocol
Ideal	No	Yes	User	User	Yes	No

Blakley & Heath "Security Design Patterns" http://www.opengroup.org/bookstore/catalog/g031.htm

ARCTEC

Towards an Ideal Proxy



	Passwd to guard1	Userid to guard2	Guard2 authn	Guard2 authz	Sso	Delegation protocol
Ideal	No	Yes	User	User	Yes	No

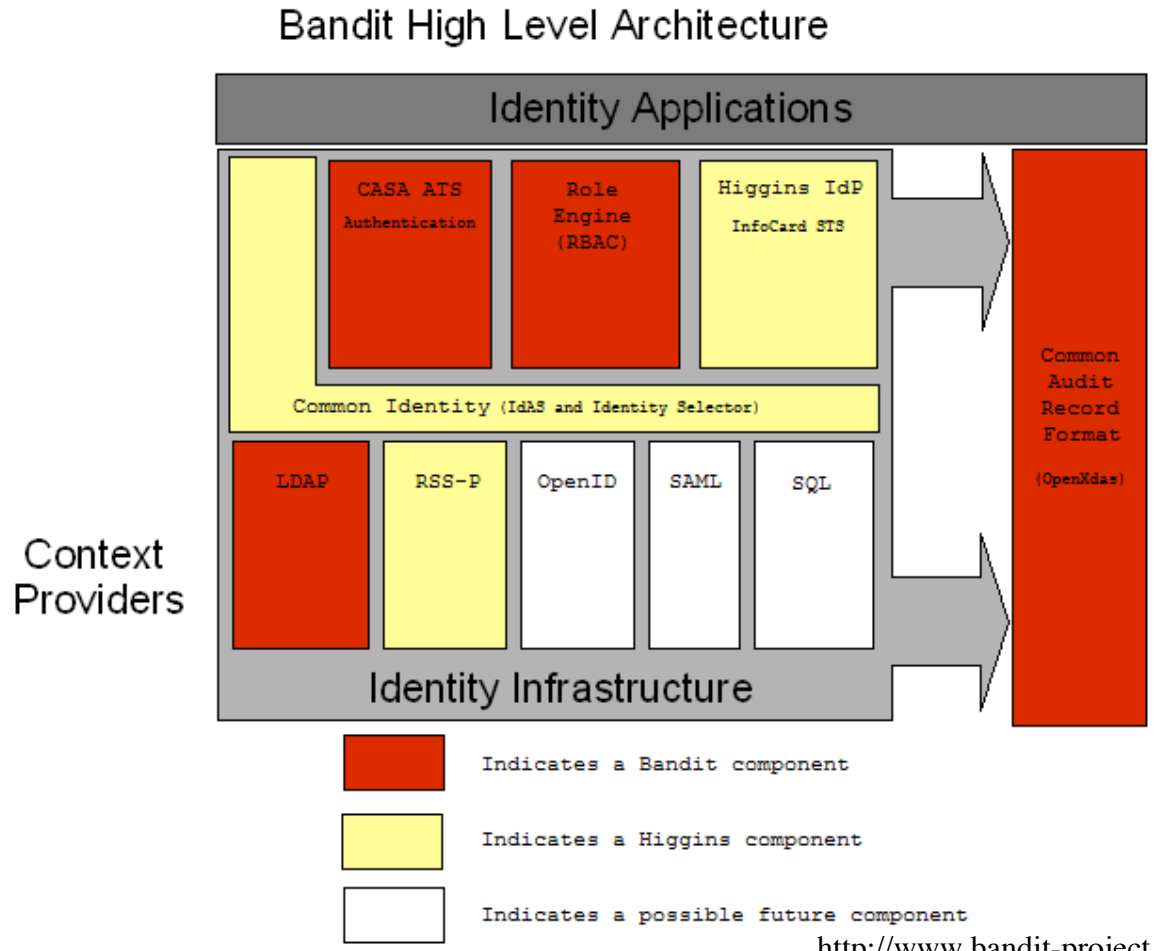
Blakley & Heath "Security Design Patterns" http://www.opengroup.org/bookstore/catalog/g031.htm

Leveraging WS-Trust

- Authentication
  - Extend reach of authentication technologies, for example 2FA
- Authorization
  - Consistent authorization policy enforcement
- Auditing
  - Central point for access control auditing
- Standards
  - Rely on open standards instead of proprietary mechanisms

ARCTEC

Bringing it all together - DigitalMe & Bandit Project



http://www.bandit-project.org/index.php/Digital_Me

ARCTEC

DigitalMe

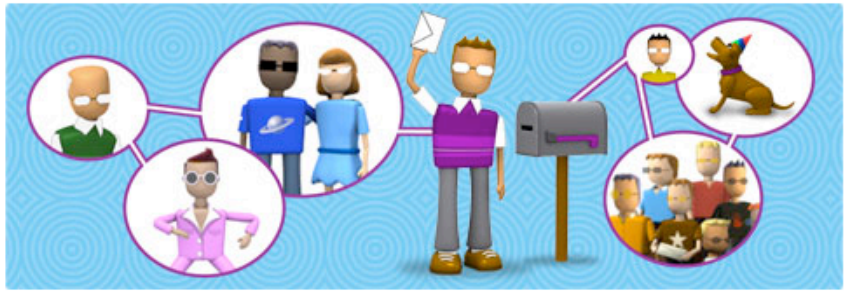
- Enable integration with InfoCard-compatible web sites and services.
- User selects card to assert credentials (instead of typing in username/password)
- The credentials and required claims are bundled into a request that is signed and sent to the STS.
- The STS extracts information from the token request, authenticates the user via the IDP, and retrieves the requested claim values. The response is bundled into a message that is signed by the STS and returned to the identity selector.
- The identity selector passes the token returned by the STS to the relying party site.
- The relying party site verifies that the token is issued by a trusted STS and that the token is valid (signature is good, token hasn't expired, etc.).
- Claim values are extracted from the token by the relying party and are used to complete the transaction.
- http://www.bandit-project.org/index.php/Digital_Me

ARCTEC

Passwords are tired

YAHOO! MAIL

Yahoo! - Help



The new Yahoo! Mail gives you more ways to connect. With everyone.

BE A BETTER CHAT FANATIC!
Chat instantly with friends online with built-in instant messaging.

BE A BETTER TEXT MASTER!
Send updates to friends on the go with integrated text messaging.

BE A BETTER JET SETTER!
Get mail whenever and wherever you want on your mobile phone.

The new Yahoo! Mail is here. See what it can do for you.

Prevent Password Theft

Sign in to Yahoo!

Yahoo! ID:

Password:

Keep me signed in
for 2 weeks unless I sign out. New!
[Uncheck if on a shared computer]

Sign In

Forget your ID or password? | Help

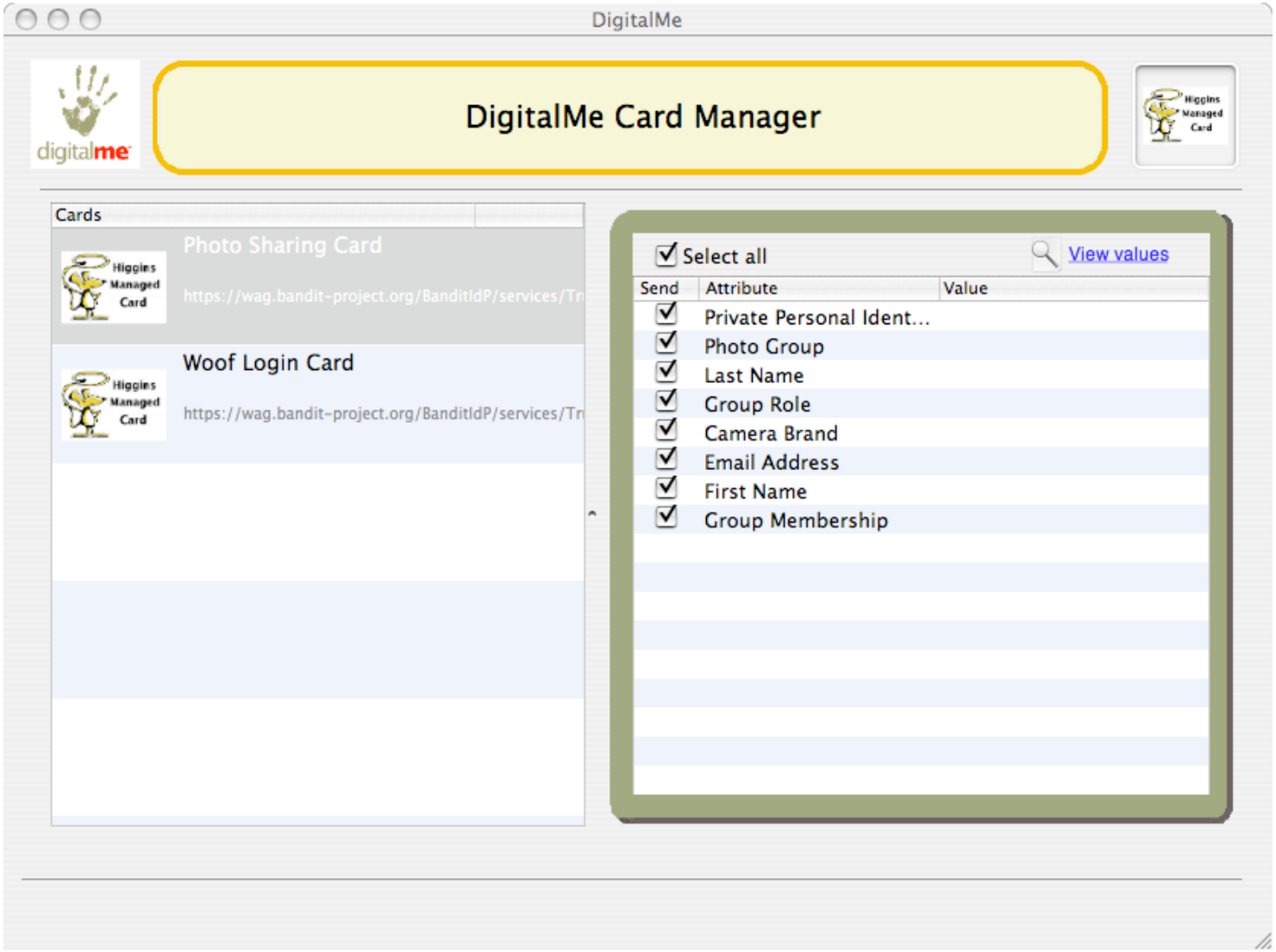
Don't have a Yahoo! ID?
Signing up is easy.

Sign Up

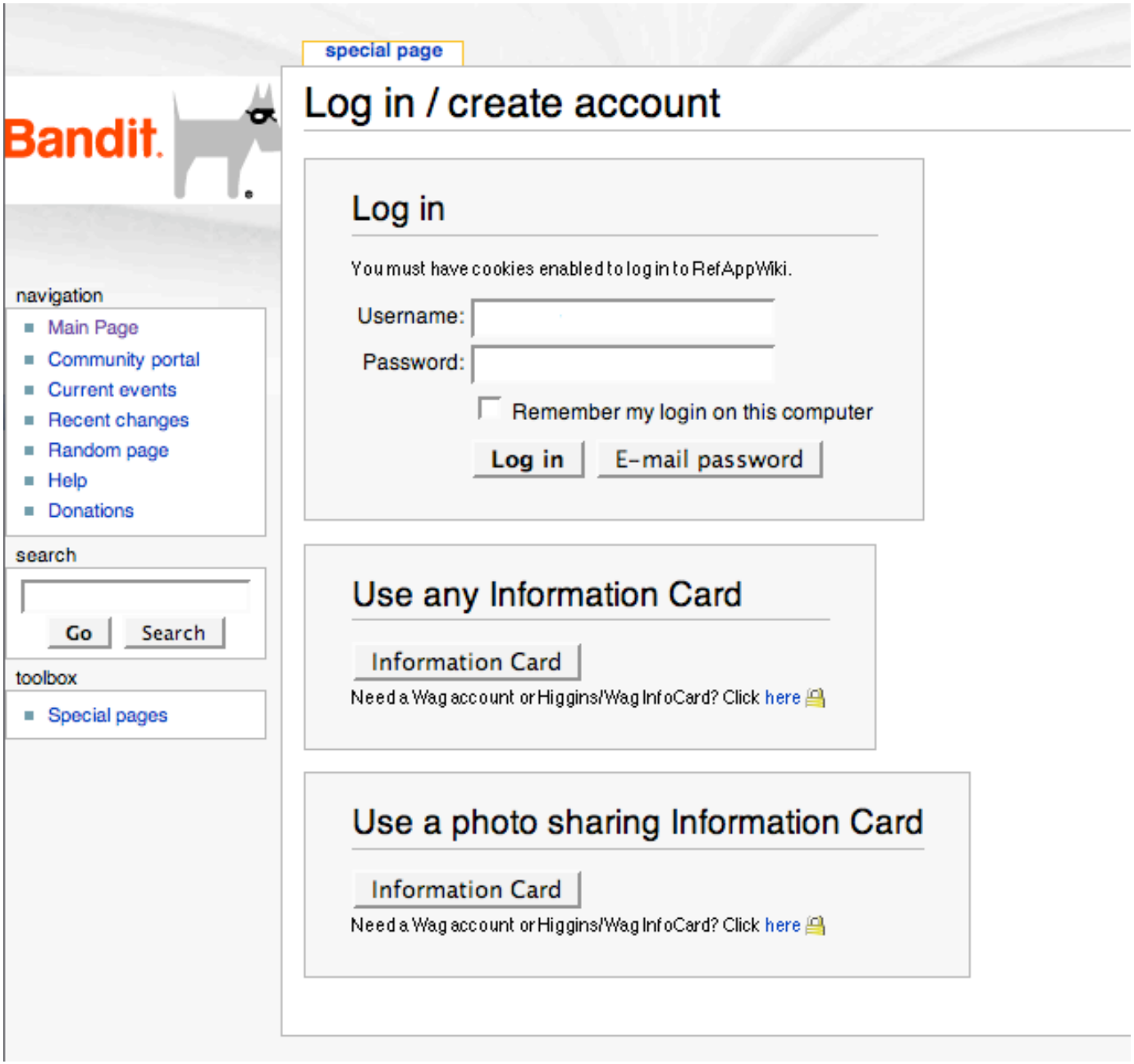
One Yahoo! ID. So much fun!
Use your single ID for everything from checking Mail to checking out Yahoo! Music, Photos, Messenger, and more.

ARCTEC

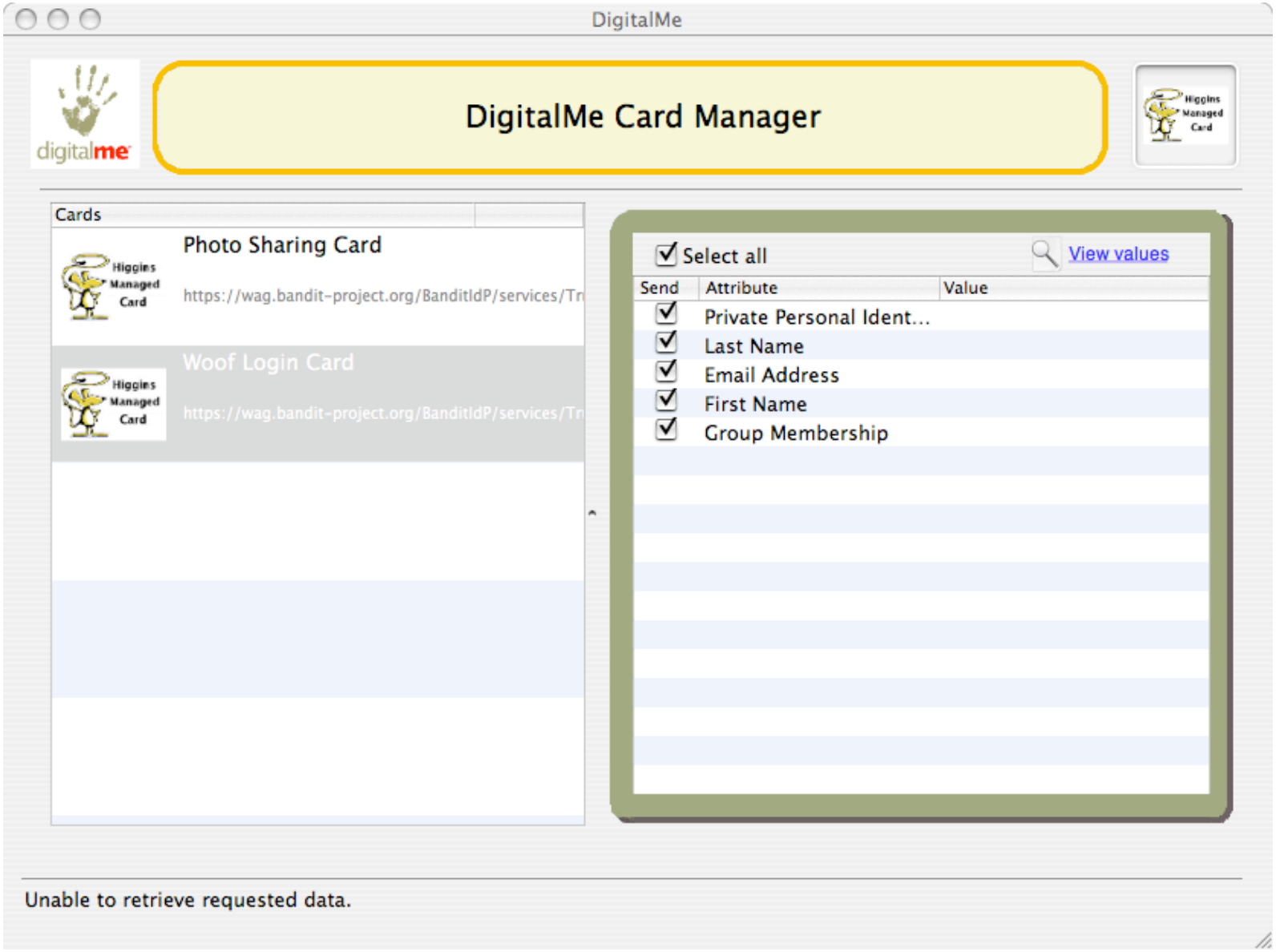
Cards are wired



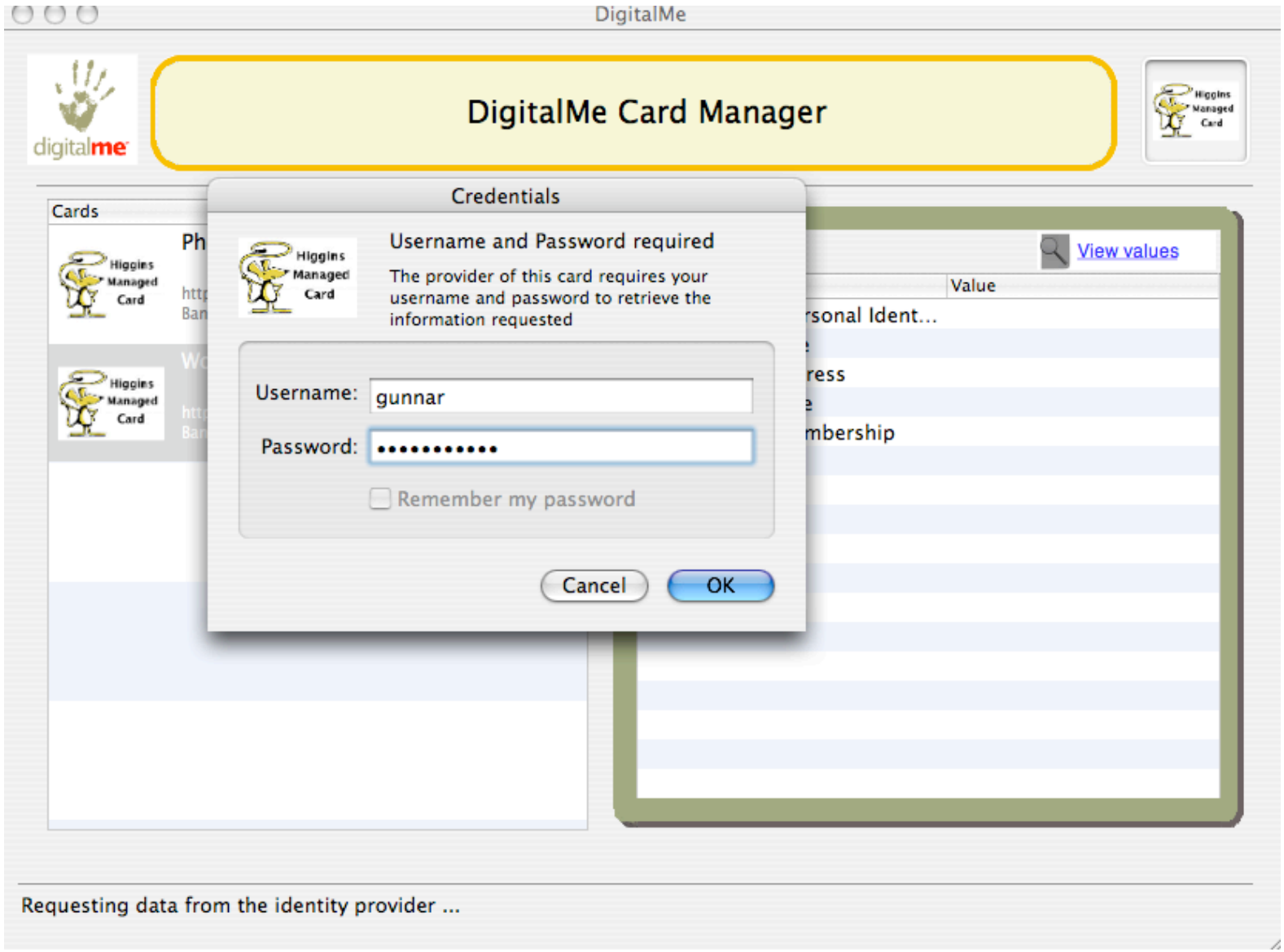
ARCTEC



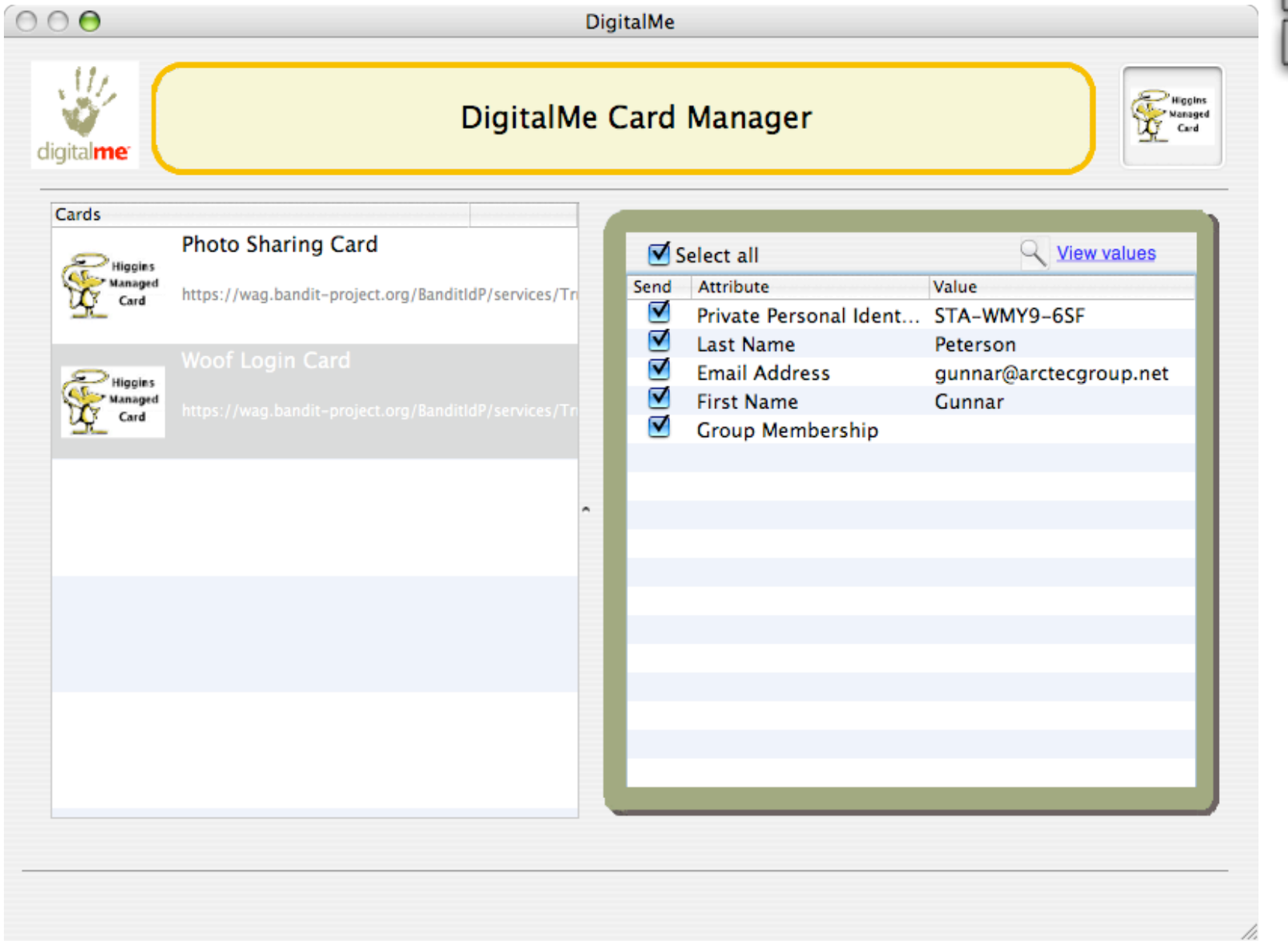
ARCTEC



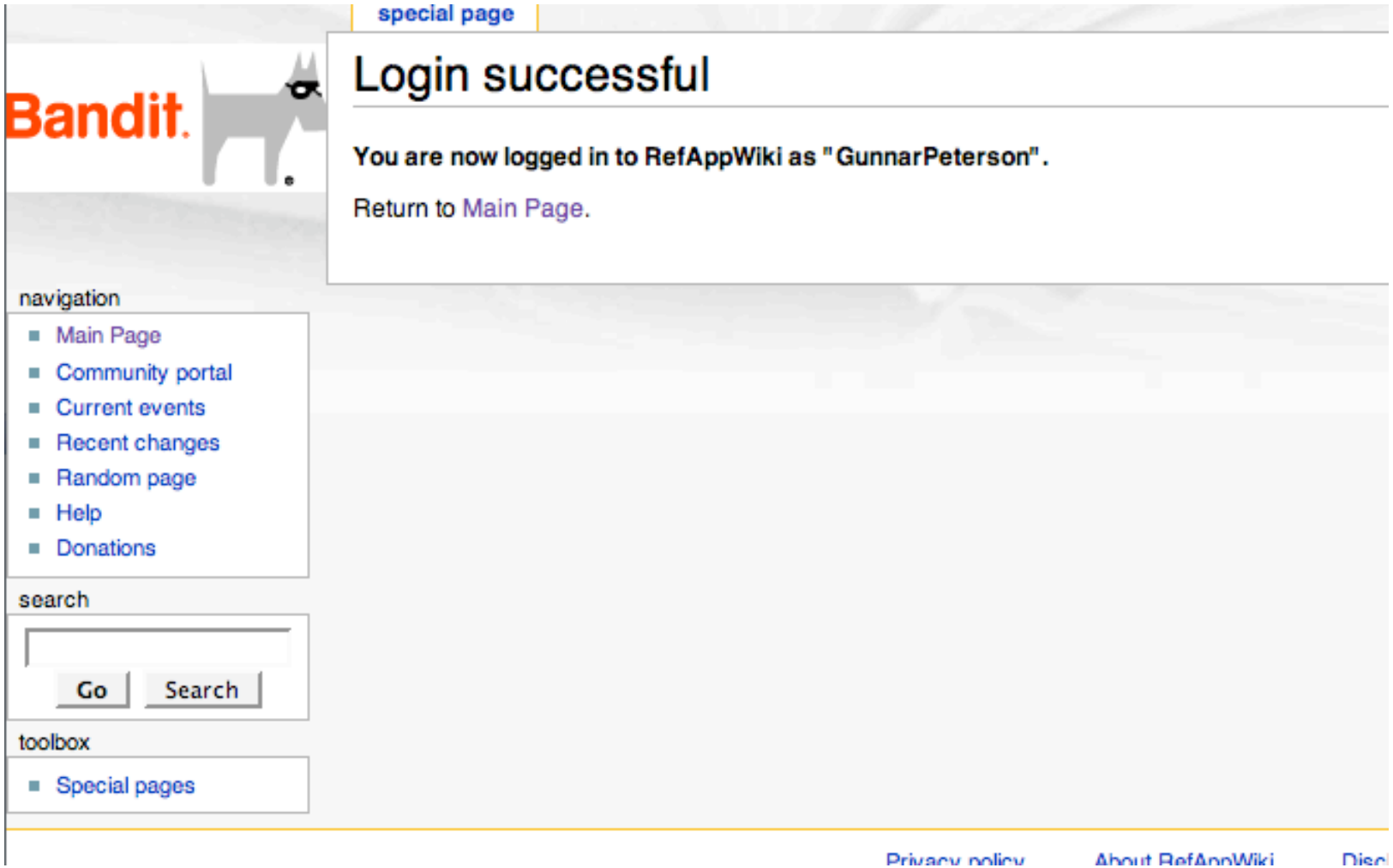
ARCTEC



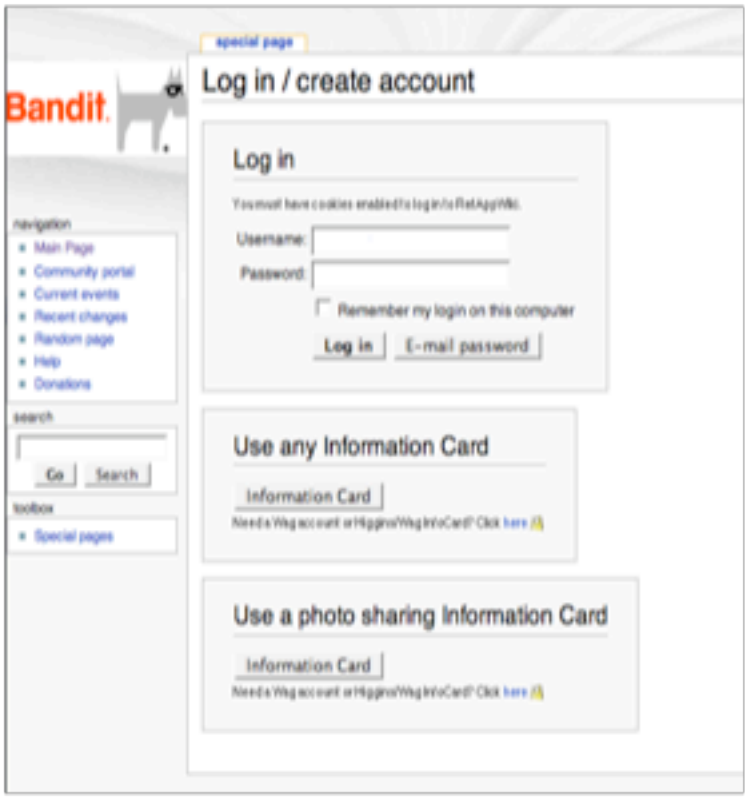
ARCTEC



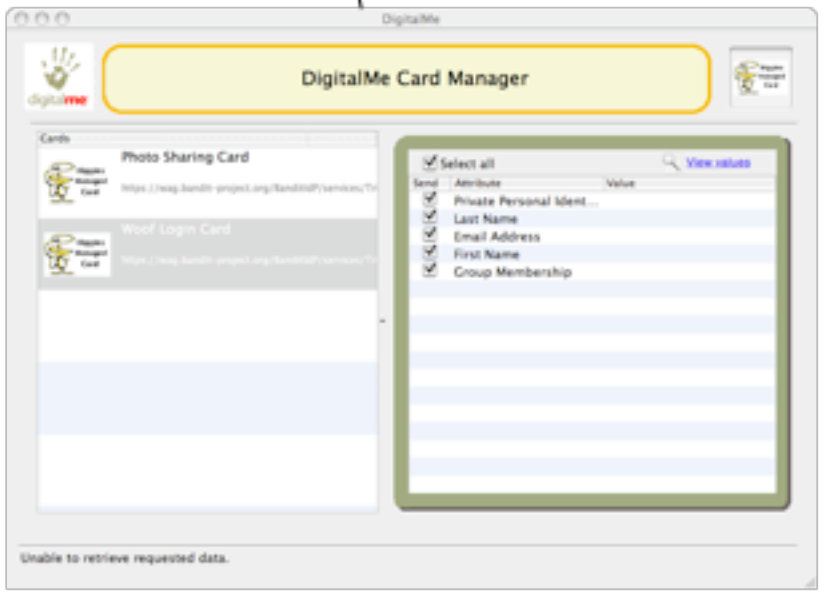
ARCTEC



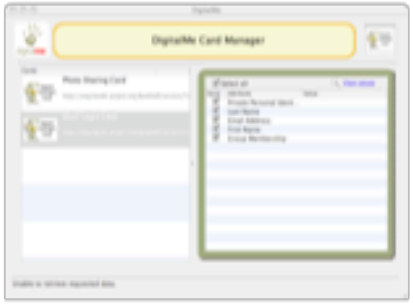
ARCTEC

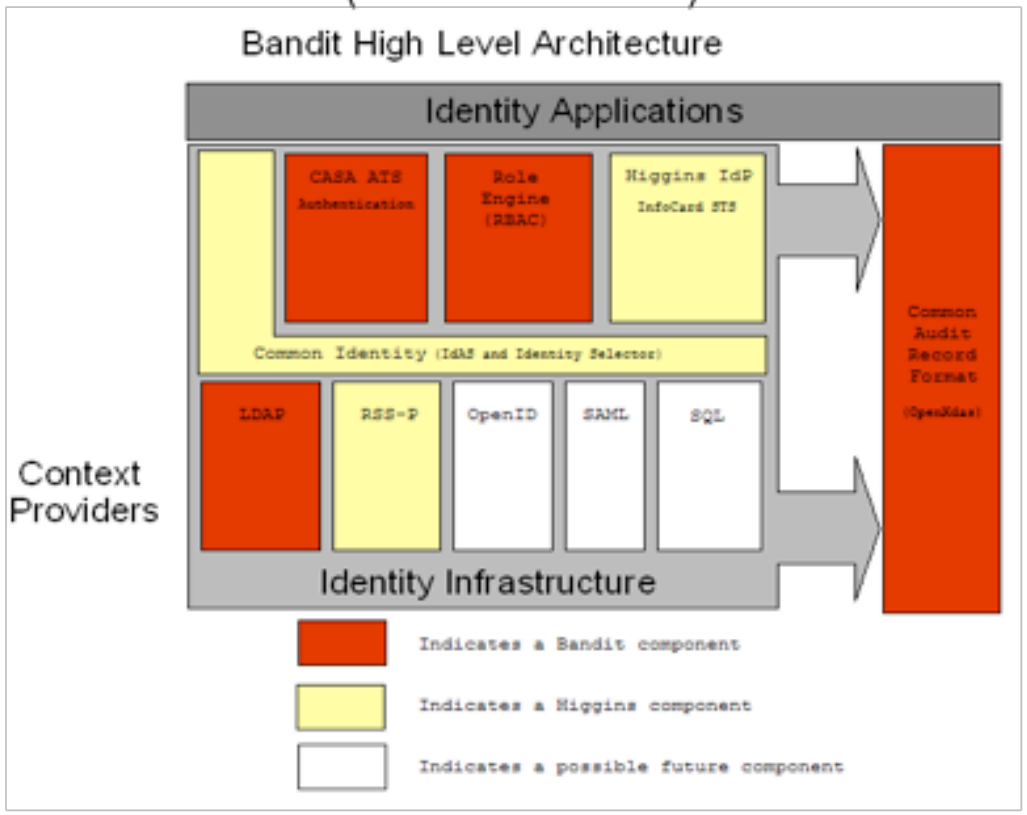


ARCTEC



ARCTEC





ARCTEC