>Applied Technology Solutions, Inc.(ApTSi™)

Applying Technology to Business Problems™

THE Open GROUP

Making standards work®

Understanding the role of security on SOA and Cloud Computing: a reference model, governance, issues and best practices

The Open Group Security Practitioners Conference, San Diego, Feb 5th, 2009

Introductions

- **Feb 5th, 2009**

ApTSi ™
Applied Technology Solutions, Inc.

• **Name**	**Title**
• Nikhil Kumar	President Co-Chair SOA Reference Architecture Project, The Open Group
•	

- **Leadership**
- **World Class Technology**
- **Experience**

- **Strategy**
- **Integration & SOA**
- **Application Development & Reuse**
- **DB, EII & BI**

Nikhil Kumar President
Email: nikhil@ap-tech-solns.com
Blog: http://blogs.ittoolbox.com/emergingtech/nikhil
Phone: (248) 797 8143

Agenda

- Modeling and addressing "traditional" SOA Security
  - Review CIA-TRIAD and AAA approach
- Security issues that arise
  - The importance of securing data at flight and rest
  - SOA issues
    - Who are we: understanding our ecosystem
    - The SOA effect – not knowing who we will be
    - In the small: at a service level
      - Key issues
        - » Trust, Authentication and Authorization
        - » Confidentiality
        - » Integrity and Non-repudiation
        - » Audit
        - » Contracts and guards
    - In the large – crossing borders
      - Federation and its implications
        - » Trust, authentication and authorization

BACK FORWARD

Agenda

- Security, SOA, SOI, Infrastructure Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

Understanding and establishing a contextual base:

Service-Oriented Architecture (SOA) has been defined by the Open Group as an architectural style that supports **service orientation.**

An **architectural style** is the combination of distinctive features in which architecture is performed or expressed.

A **service**:

- Is a logical representation of a repeatable business activity that has a specified outcome (e.g., check customer credit; provide weather data, consolidate drilling reports)
- Is self-contained
- *May be* composed of other services
- Is a "black box" to consumers of the service

There are multiple perspectives of SOA which address it from a business context, where organizations align themselves and their value chain around a service centric model (the Service Oriented Enterprise), a technical and operational context and from a governance context

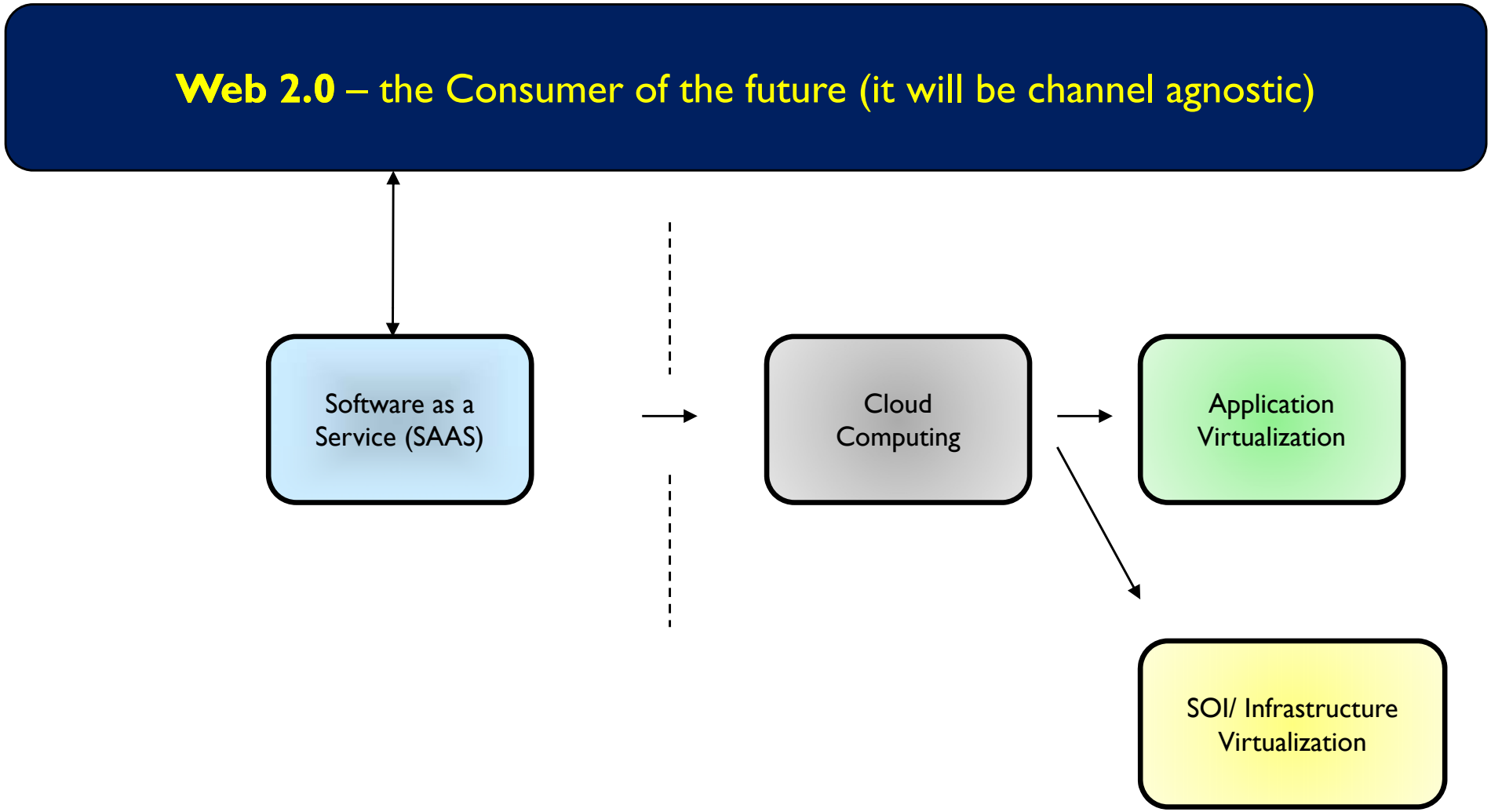
It is important to take these 3 perspectives (business, technology and governance) into consideration to be able to understand the implications of SOA

Shared Services, SaaS, Cloud Computing, SOI and Infrastructure Virtualization are all extensions of SOA, and represent the natural evolution of SOA. On the next slide we describe these terms and complete with a review of the evolution of SOA

BACK FORWARD

The future services ecosystem

SOA 2.0



Understanding and establishing a contextual base – the new SOA

Shared Services are services which are shared (used) by other services. Attributes which delineate them Include reuse, agility, fiscal governance, decision right and ownership issues, quality of service, security, privacy and compliance issues, provisioning and interoperability being more important than single, one-time used services

Software As A Service – Software as a service occurs when organizations define business process and core capabilities in terms of a service. These services can then be provided by any service provider.

- These services are inherently services which are shared, and all of the above attributes of shared services apply.
- Software as a service may be provided by either elements within an enterprise or across enterprise domains. The perimeter is rapidly becoming meaningless.
- The most compelling aspect of SaaS is the agility and cost reduction that arises.
- SaaS represents the true *commoditization of IT.*
- *The **Business Implications** are extraordinary.*

Understanding and establishing a contextual base – the new SOA

Service Oriented Infrastructure (SOI) and Infrastructure Virtualization:
Service Oriented Infrastructure is the definition of key infrastructural capabilities in a service oriented manner and the supporting attributes that infrastructure may be involved.

Infrastructural Virtualization is the process of providing infrastructure in a virtualized manner, where the location of the infrastructure and the environment that it runs in are theoretically unimportant to the user. Important characteristics include:

- The categorization of the virtualized infrastructure into "physical infrastructure" – such as operating systems and hardware, and "application infrastructure" – such as "cloud application servers"
- The governance of the information, the data and the services – at all levels

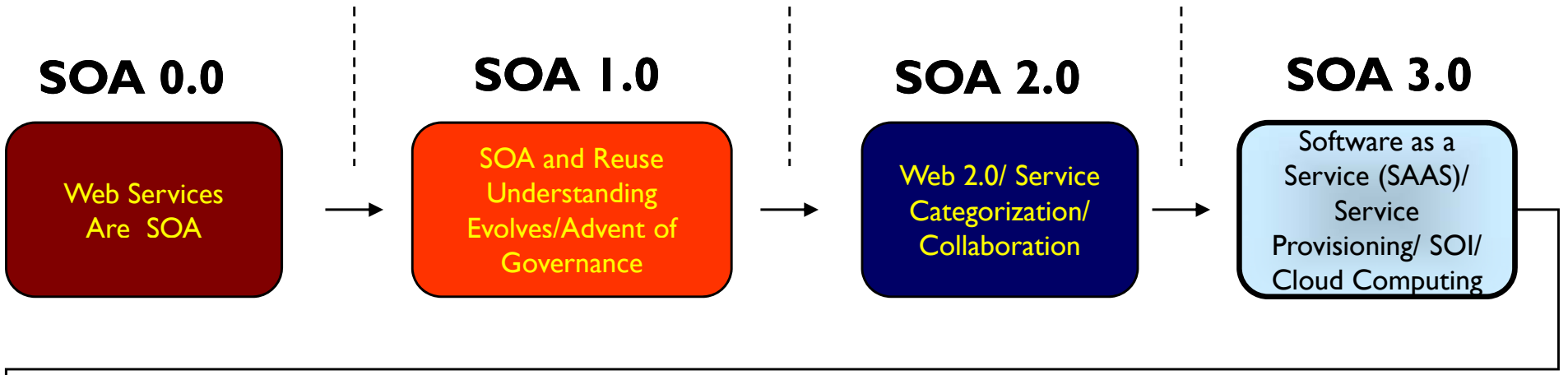
Cloud Computing: is the running of services in a virtualized fashion in a cloud – including other business services as the other two categories described above – application services and infrastructure services

Web 2.0: Web 2.0 can be envisioned as the consumer layer of these capabilities that represent the future. The other capabilities provide the underlying basis for this. There are domain specific and societal implications of Web 2.0, with new business models and new roles

BACK FORWARD

Wither now? The Future and the Present

SOA Evolution



Security Implications

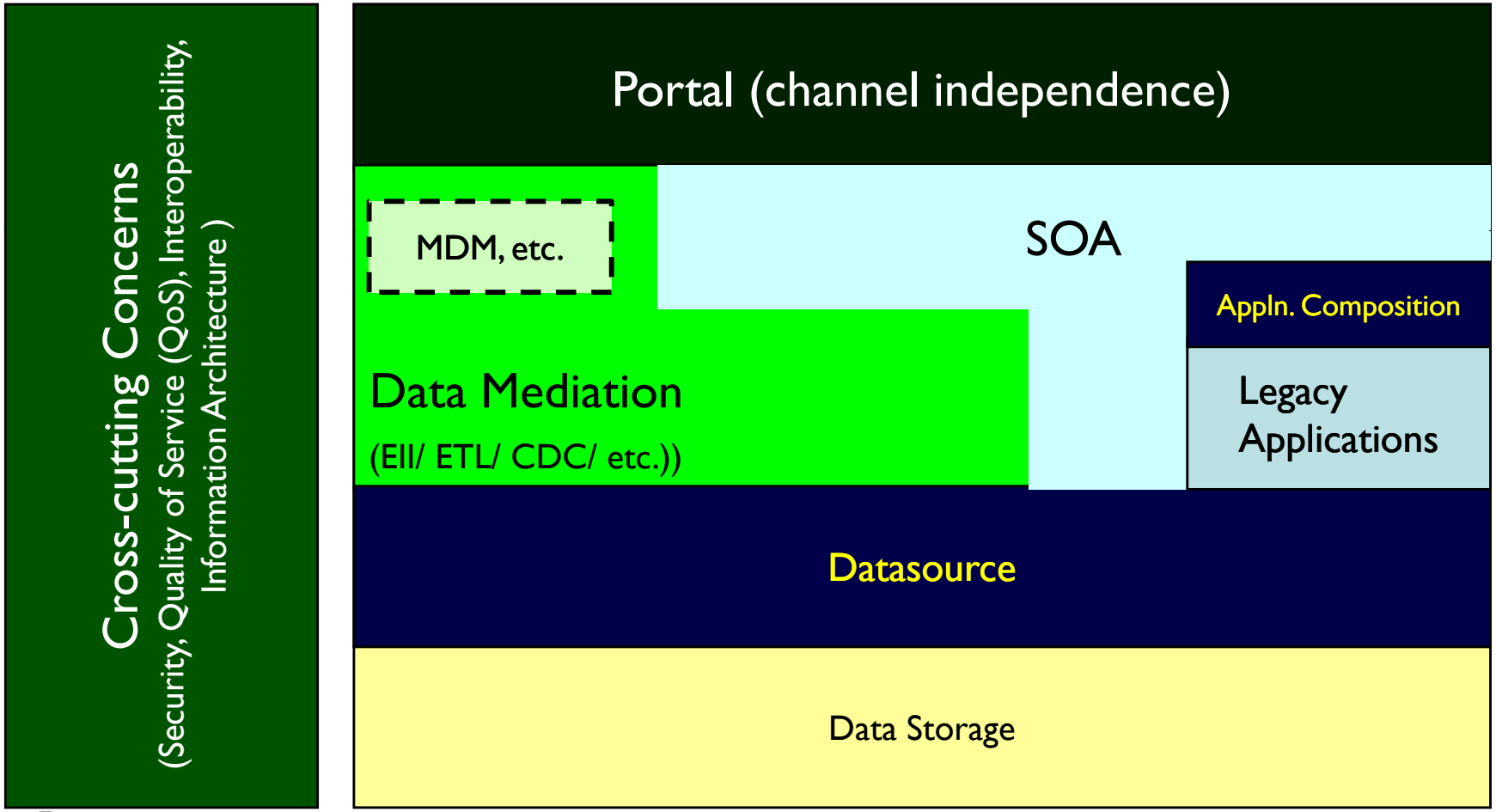
- Web 2.0 → The shareability of data/ absence of perimeters/ data tracking in long-tail scenarios, the impact of mashups and technologies such as AJAX
- Service Categorization → The impact of service shareabiltiy and the impact of header information on the data
- Collaboration → the creation of composed and orchestrated solutions. Security impacts include the impact of composition and the associated privileges of the composed or collaborating services
- SAAS → Interoperability, Security and Compliance, QoS and Temporal differences, Coupling and dependencies
- SOI → Data Integrity, Interoperability impact of platforms and SOI solutions (e.g. impact of ACE-ML)
- Cloud Computing → Portability, vendor independence, scalability, QoS and governance, security, compliance, loss of the perimeter

Agenda

- Security, SOA, SOI, Infrastructure Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

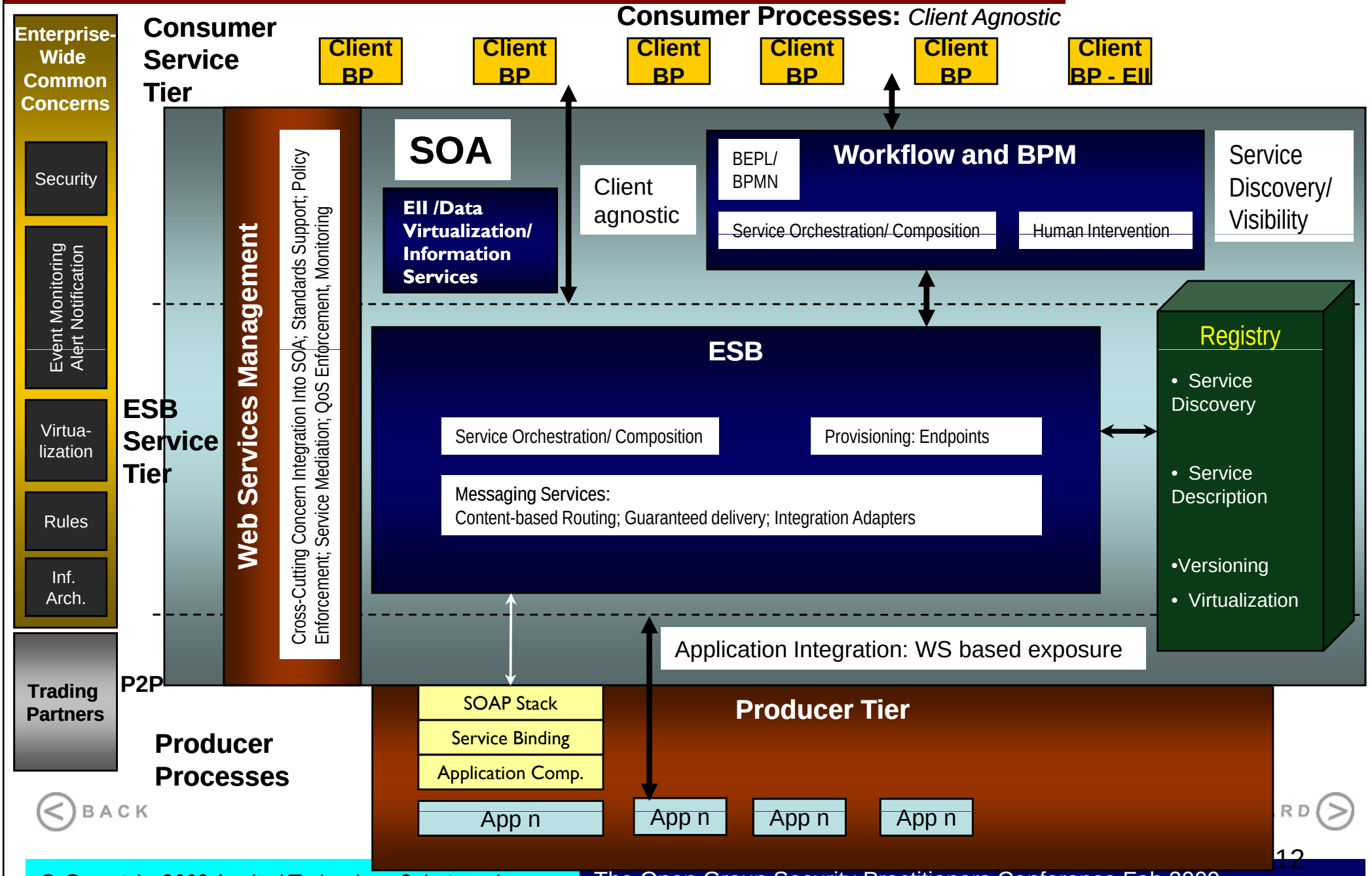
Future State "Actionable Architecture ™ Reference Model: Deployment Layers in the Runtime

The **Actionable Architecture ™** of the future will support a channel independent structure that will support varying sources of data, drive unified data views, be interoperable and service oriented and apply application composition to wrap legacy solutions into future state services .



BACK
FORWARD

SOA Reference Model: Layers and Responsibilities for a Run Time SOA Architecture

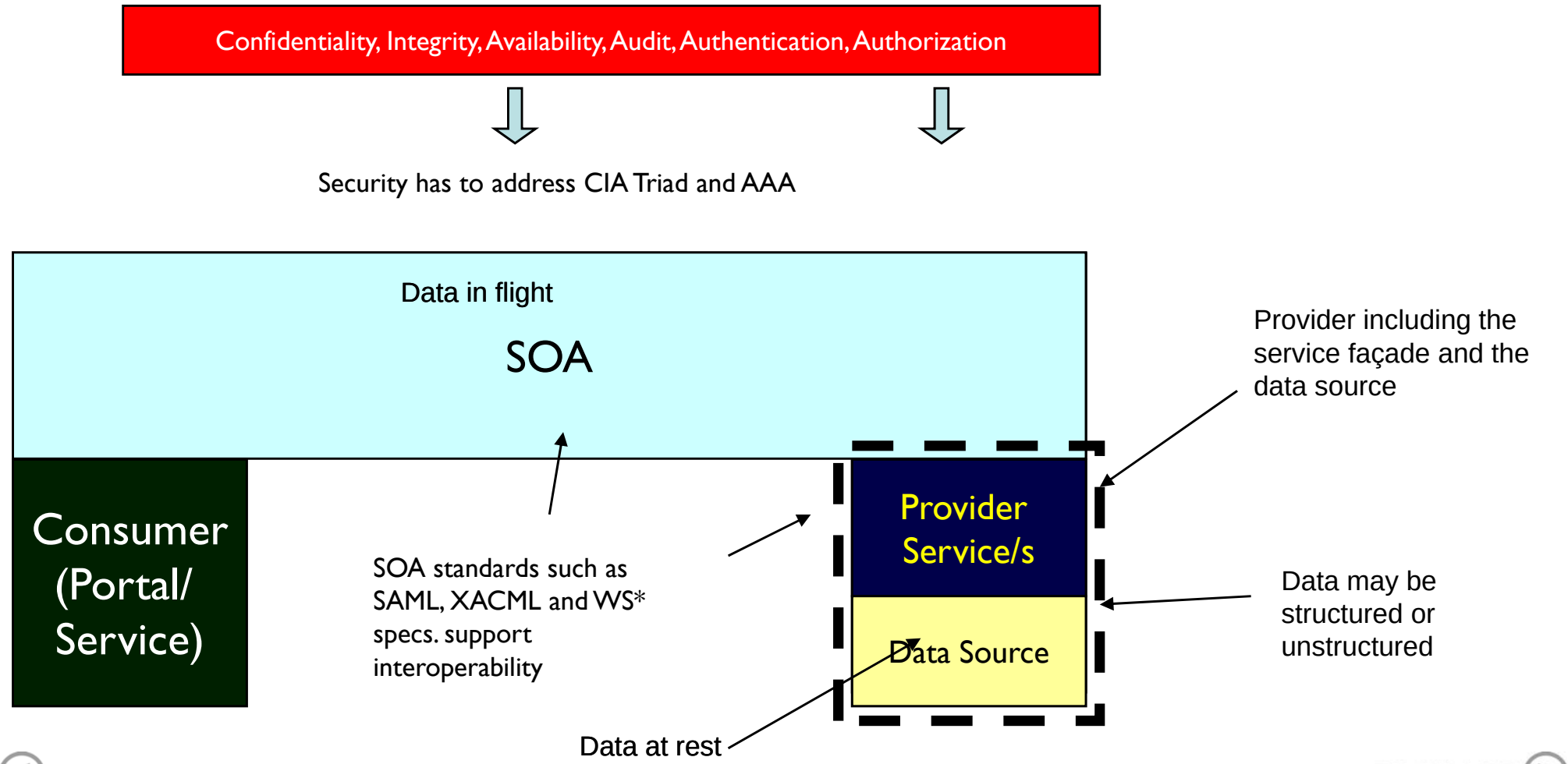


The Security Reference Model: applied to ApTSi's Actionable Enterprise Architecture

Security needs to address the flow of data across the SOA. This includes data at rest and data in flight.

Cross-cutting security constraints:

Security Constraints apply across all layers of a consumer producer interaction

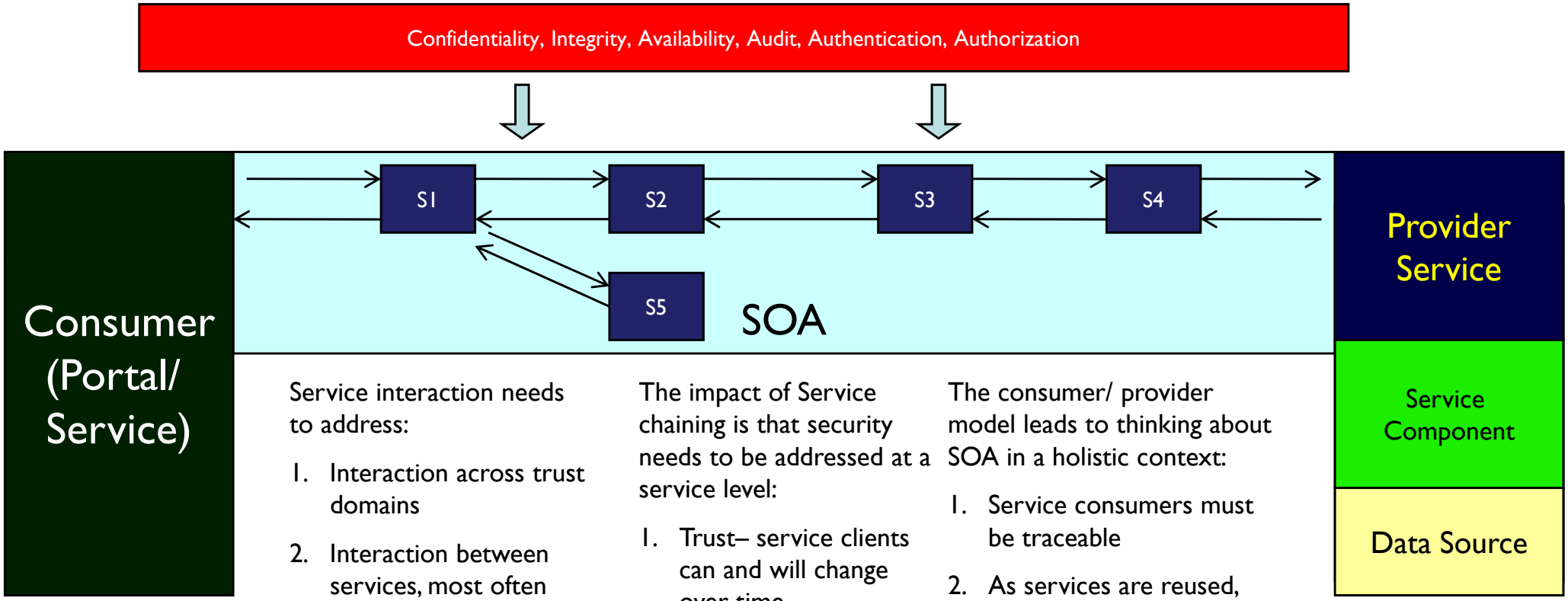


Service interaction, Chaining and Composition in a runtime SOA environment

Security needs to address the flow of data across the SOA. This includes data at rest and data in flight.

Cross-cutting security:

Security is a cross-cutting constraint



Service interaction needs to address:

1. Interaction across trust domains
2. Interaction between services, most often due to the chaining of services
3. Possibilities of varying consumer and provider lists

The impact of Service chaining is that security needs to be addressed at a service level:

1. Trust– service clients can and will change over time
2. Authorization
3. Audit
4. Possibilities of varying consumer and provider lists

The consumer/ provider model leads to thinking about SOA in a holistic context:

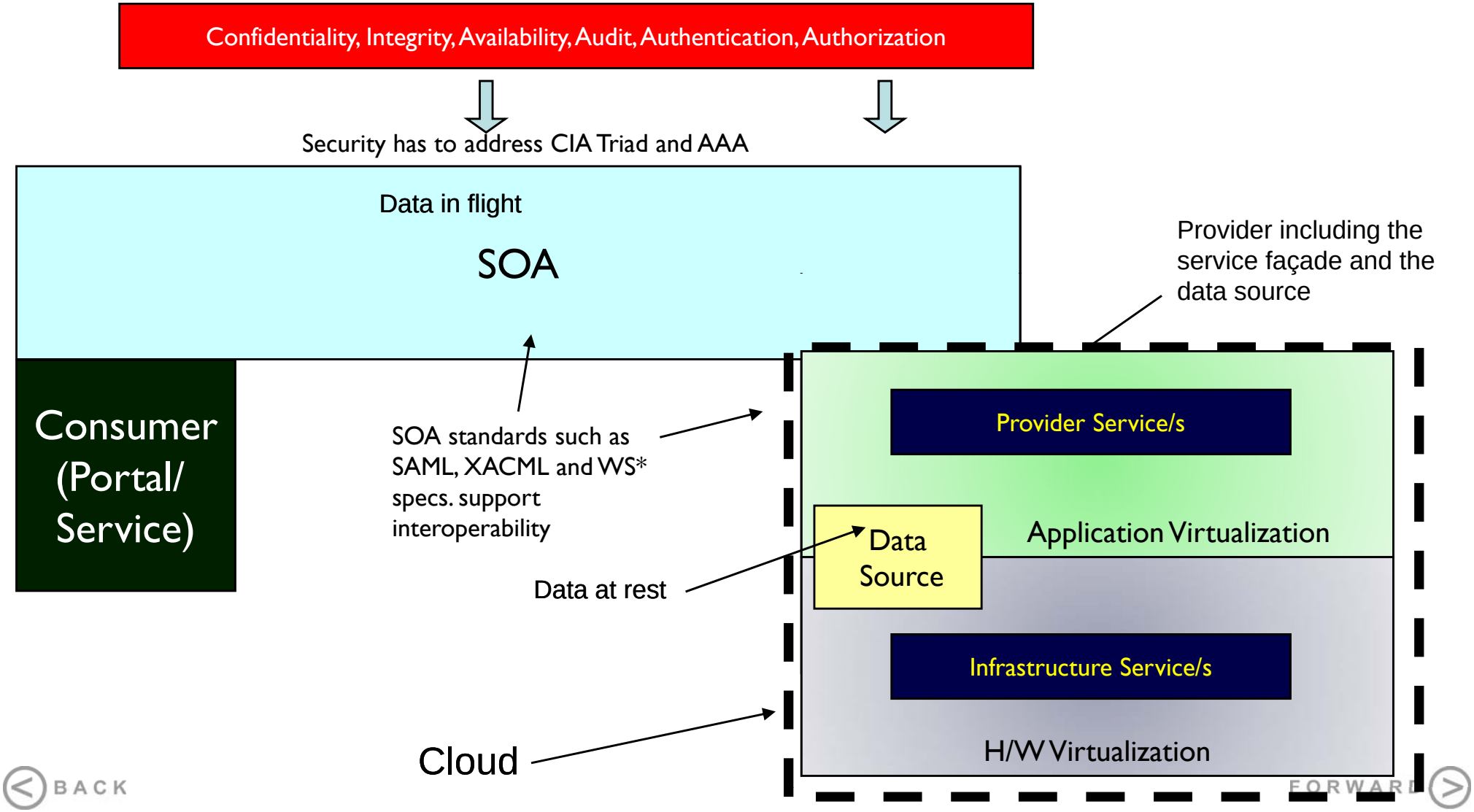
1. Service consumers must be traceable
2. As services are reused, there should not be tight coupling between a consumer and a producer.
3. Providers and the underlying data sources also have contractual commitments

BACK FORWARD

The Security Reference Model: applied to ApTSi's Actionable Enterprise Architecture: Future state scenarios (the Cloud, SOI and Infrastructure Virtualization)

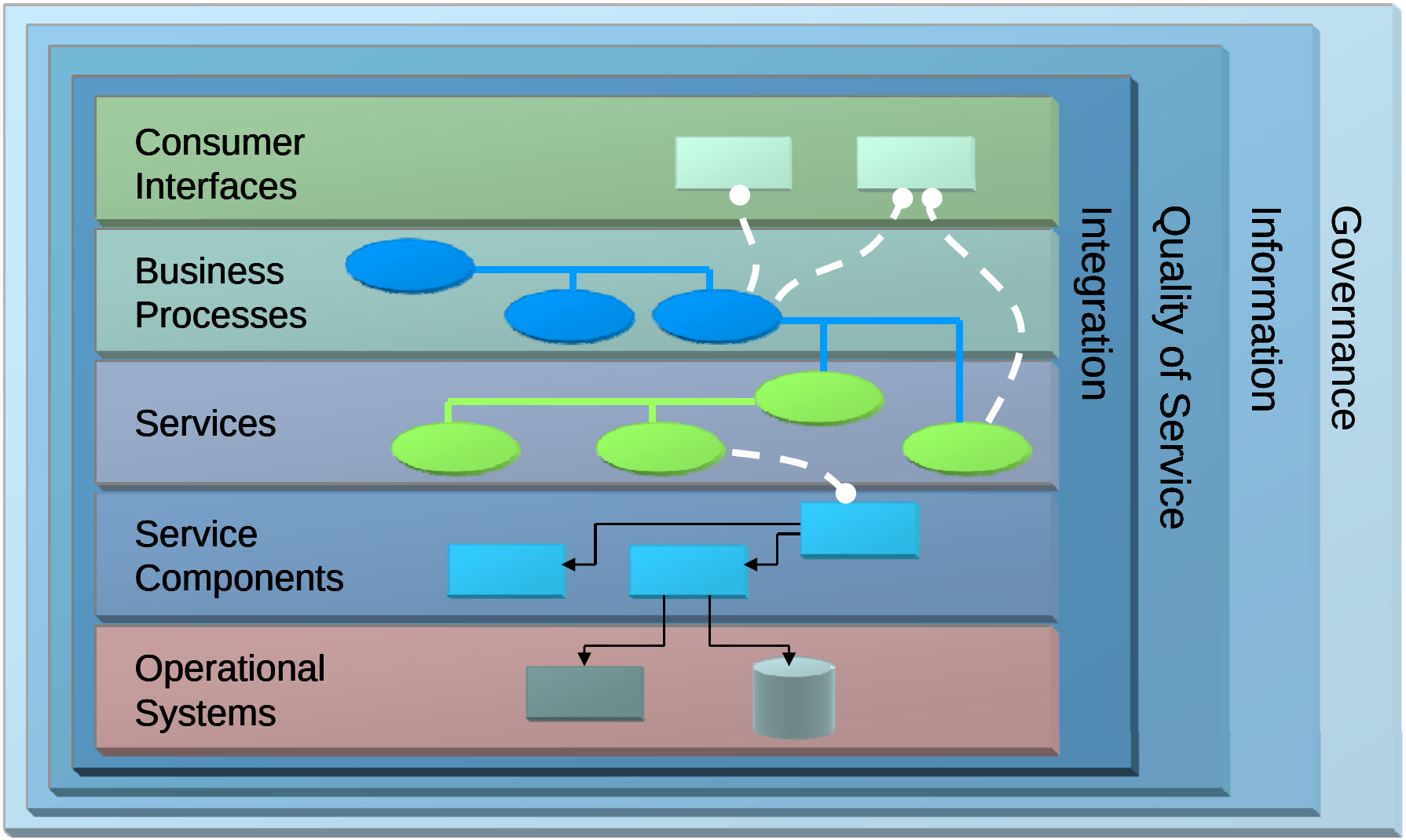
Cross-cutting security constraints:

Security Constraints apply across all layers of a consumer producer interaction



BACK FORWARD

The Open Group SOA RA – High-Level Perspective



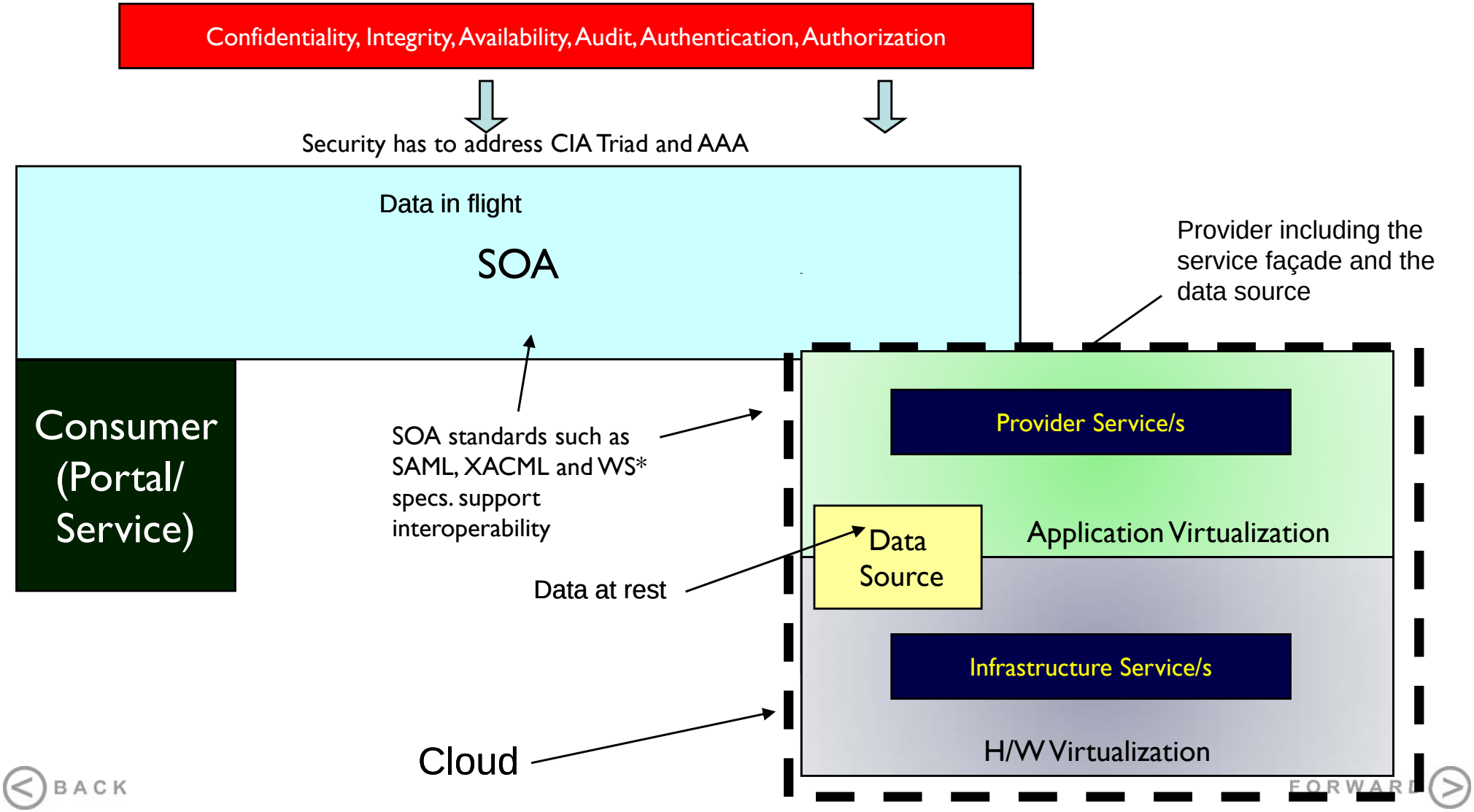
Agenda

- Security, SOA, SOI, Infrastructure Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

The Security Reference Model: applied to ApTSi's Actionable Enterprise Architecture: Future state scenarios (the Cloud, SOI and Infrastructure Virtualization)

Cross-cutting security constraints:

Security Constraints apply across all layers of a consumer producer interaction



BACK FORWARD

Modeling and Addressing "Traditional" SOA Security

Apply the CIA Triad and AAA:

- Security at the Service Level:
  - Address the transport
    - Non-repudiation
    - Integrity
    - Encryption
  - Address the potential for storage
  - Make it atomic
- Security and Availability
  - QoS
- Security at the Service Level
  - Understand the data
  - Understand the security constraints supported by the service
    - Model the constraints as a part of the service contract
    - Ensure that they are enforceable in the for of rule

Modeling and Addressing "Traditional" SOA Security

Apply the CIA Triad and AAA:

- Confidentiality
  - How are the service contract and service pre-conditions supporting confidentiality?
  - What is the role of the supporting elements of the SOA?
    - » How does this impact the physical interaction including the transport medium?
    - » How does this impact? <?>
  - How does this impact the Service?
    - » Its role in the post-conditions that the service is committed to conform to
    - » Its role in the pre-conditions that the consumer's request must be validated against
  - How does this impact the service provider (the *service component*)?

- Non-repudiation
  - Try and establish a consistent framework which cross-cuts from an enterprise perspective
  - Use a data-classification strategy to help determine the level and nature of non-repudiation required
  - Add it to the SOA strategy and governance frameworks
  - Ensure that there is a review and design process at a service level from the perspective of ensuring that non-repudiation is assured across the SOA continuum.

BACK FORWARD

Modeling and Addressing "Traditional" SOA Security

Apply the CIA Triad and AAA:

- Integrity
  - Establish transaction integrity classification. This may be driven by standards (for example Sarbanes Oxley 404) and will normally need to address both data at rest and in flight.
  - Look to data classification to create a framework for SOA
  - In the design guidance framework ensure that the entire service chain addresses integrity. Integrity translates to encryption and non-repudiation as we try to ensure that the data traversing from a service provider to a service consumer stays valid.

- Availability:
  - From the SOA strategy process where capabilities are defined and infrastructure determined
  - From the SOA design process
  - From the operationalization process
  - From the run-time monitoring process.

BACK FORWARD

Modeling and Addressing "Traditional" SOA Security

Apply the CIA Triad and AAA:

- Authentication (and trust establishment)
  - Federated and non-federated scenarios
  - Distribution of the trust assertion and federation
- Authorization
  - Entitlements
  - Content level entitlements
  - Policies and PEP's
  - Validate the consumer
  - Entitlements based on data levels
- Audit
  - Know who started the chain and the consumer
  - Obfuscate some data

Agenda

- Security, SOA, SOI, Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

Agenda

- Security issues that arise
  - The importance of securing data at flight and rest
  - SOA issues
    - Who are we: understanding our ecosystem
    - The SOA effect – not knowing who we will be
    - In the small: at a service level
      - Key issues
        - » Trust, Authentication and Authorization
        - » Confidentiality
        - » Integrity and Non-repudiation
        - » Audit
        - » Contracts and guards

Agenda

- Security issues that arise
  - SOA issues
    - In the large – crossing borders
      - Federation and its implications
        - » Trust, authentication and authorization
        - » Identity and its role (refer to Stuart and Dennis's presentation)
        - » Contract implications
        - » Remember the message

Agenda

- Security issues that arise
  - The importance of securing data at flight and rest
  - SOA issues
    - Audit and its opportunity
      - What do I audit
      - What do I obfuscate?
      - Do I lose my integrity?
  - Maturity and its impact
    - You plan your SOA rollout, so why don't you tie your security rollout there too
    - So how about dancing? Learn the fandango!
  - Security and Service contracts

Agenda

- Security, SOA, SOI, Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

SAAS and its Implications

- Federation
  - ID Management
  - Trust
  - Levels of trust
- Change Impact – when Providers Change
- Service Chaining and not knowing who is providing the information
- New Versions

SOI and Infrastructure Virtualization

- Security, SOA, SOI, Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

SOI and Infrastructure Virtualization

- Application Virtualization
  - Where does the Application Run?
  - What happens when it crashes – DR and Availability
  - What happens when it changes?
  - Can I trust my neighbor?

- Infrastructure Virtualization
  - Similar Questions
  - Need to manage securely how we access
  - Need to manage data at rest
  - Need to be careful of how we integrate

SOI and Infrastructure Virtualization

- Security, SOA, SOI, Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

Address the Cloud

- The issues of Application and Infrastructure Virtualization apply
- When we deal with the cloud the entire deployment process is an issue
- Access of the resources is an issue
- Data needs to be doubly secure
- Audit data still needs to be captured

SOI and Infrastructure Virtualization

- Security, SOA, SOI, Virtualization, Software as a Service and the Cloud
- A Reference Model for SOA Security
- Modeling and addressing “traditional” SOA Security
- Security issues that arise
- SaaS and its implications
- SOI and Infrastructure Virtualization
- Address the cloud
- Governance and Security
- Summary and Conclusions

SOA Security Governance: Topics to cover

- Strategic Governance
- Portfolio Management
- Development Lifecycle Governance
- Operationalization Governance
- Metrics and Compliance

Security for SOA: The Current and the Future

Defining issues for current state SOA

1. Security from a data at rest and a data in flight perspective
2. Understanding service security within the context of a service
    1. The service contract
    2. Physical interface level security
3. Understanding service security within the context of a service chain (orchestration/ composition scenarios)
4. Audit implications

Defining issues for current state SOA

1. The evolution of circles of trust, information architecture and multiple service environments
2. Focused on system requirements
    1. Interoperability at a system level
    2. Data Model is the vehicle for communication
3. Normally deals with persistence and not transport of data

Conclusion

Understanding the role of security on SOA and Cloud Computing: a reference model, governance, issues and best practices

What we have covered

1. *Background and Understanding*
2. *Key Elements of SOA Security and some issues associated with SAAS/ Cloud*

Not Covered

1. *Patterns*
2. *TOGAF*

Thank you!

Thank you!

ApTSi ™
Applied Technology Solutions, Inc.

- **Feb 5th, 2009**

Name	**Title**
Nikhil Kumar	President Co-Chair SOA Reference Architecture Project, The Open Group

- **Leadership**
- **World Class Technology**
- **Experience**

- **Strategy**
- **Integration & SOA**
- **Application Development & Reuse**
- **DB, EII & BI**

Nikhil Kumar President
Email: nikhil@ap-tech-solns.com
Blog: http://blogs.ittoolbox.com/emergingtech/nikhil
Phone: (248) 797 8143