Service Oriented Networks – Security

David Brossard, M.Eng, SCEA
Senior Security Researcher, BT Innovate
Globecom 2008

While empowering new business models, SON leads to a proliferation of "application networks" and a need to adapt security policy and the way we enforce it depending on the context of interactions …

BT

… they also increase uncertainty regarding the trustworthiness of the communication channel, the virtual identities and other security assertions used and the compliance of policies and transformations enforced by the information processing components.

BT

Primary Implications of SON – Issues

- Pervasive Enterprise → mobile workforce, disappearing perimeter between the distributed enterprise and its customers
- Application Integration across the supply chain → manage the secure exposure, consumption, and composition of applications
- Compliance → Globalisation means complying with a mesh of laws & directives – evidence of compliance may be required
- e2e Operations Management → distributed services and operations render management complex
- Distributed Policy Enforcement → policies are enforced in a coordinated fashion on several points across the SOI
- Distributed Policy Management → policies authored by different administrative authorities are enforced on the same points
- Common Capabilities → infrastructure capabilities offered as network configurable services; new interaction / integration patterns; new dynamic, flexible security mechanisms with zero downtime
- New security threats → due to the new business model ; due to the Web services / Web 2.0 technology ; identify threats and address them

BT

Primary Implications of SON – Answers

- Pervasive Enterprise → secure communication layer that integrates identity management, AuthZ, auditing, real-time business intelligence…
- Application Integration across the supply chain → Secure end-to-end B2B2C / B2B2G transactions & consolidation of security standards for application networking
- Compliance → policy management and enforcement adapts to context; collection of evidence of policy enforcement to assure compliance
- e2e Operations Management → SON security dashboard shows real-time state of the corporate infrastructure including the B2B integration points
- Distributed Policy Enforcement → Policy-driven, customisable, remotely managed Security Appliances for the application layer
- Distributed Policy Management → Support for multiple administrative authorities, constrained delegation and non-repudiation of policy issuance
- Common Capabilities → Context-driven integration of network services; content-rich communication & Secure metadata transformation
- New security threats → Policy analysis and validation; security gateways that protects against common XML threats e.g. node depth, schema

BT

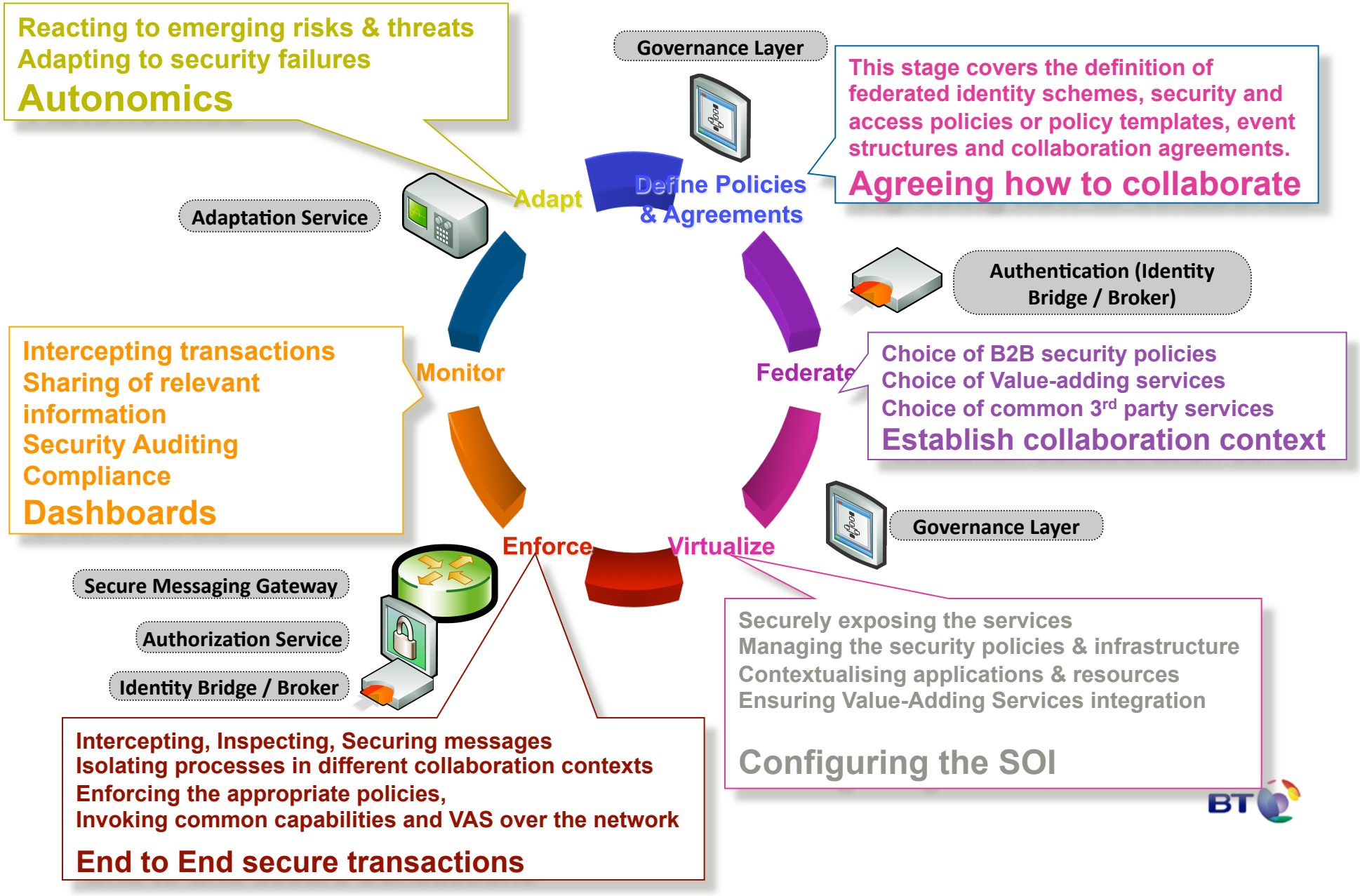
We need to provide a flexible security infrastructure where

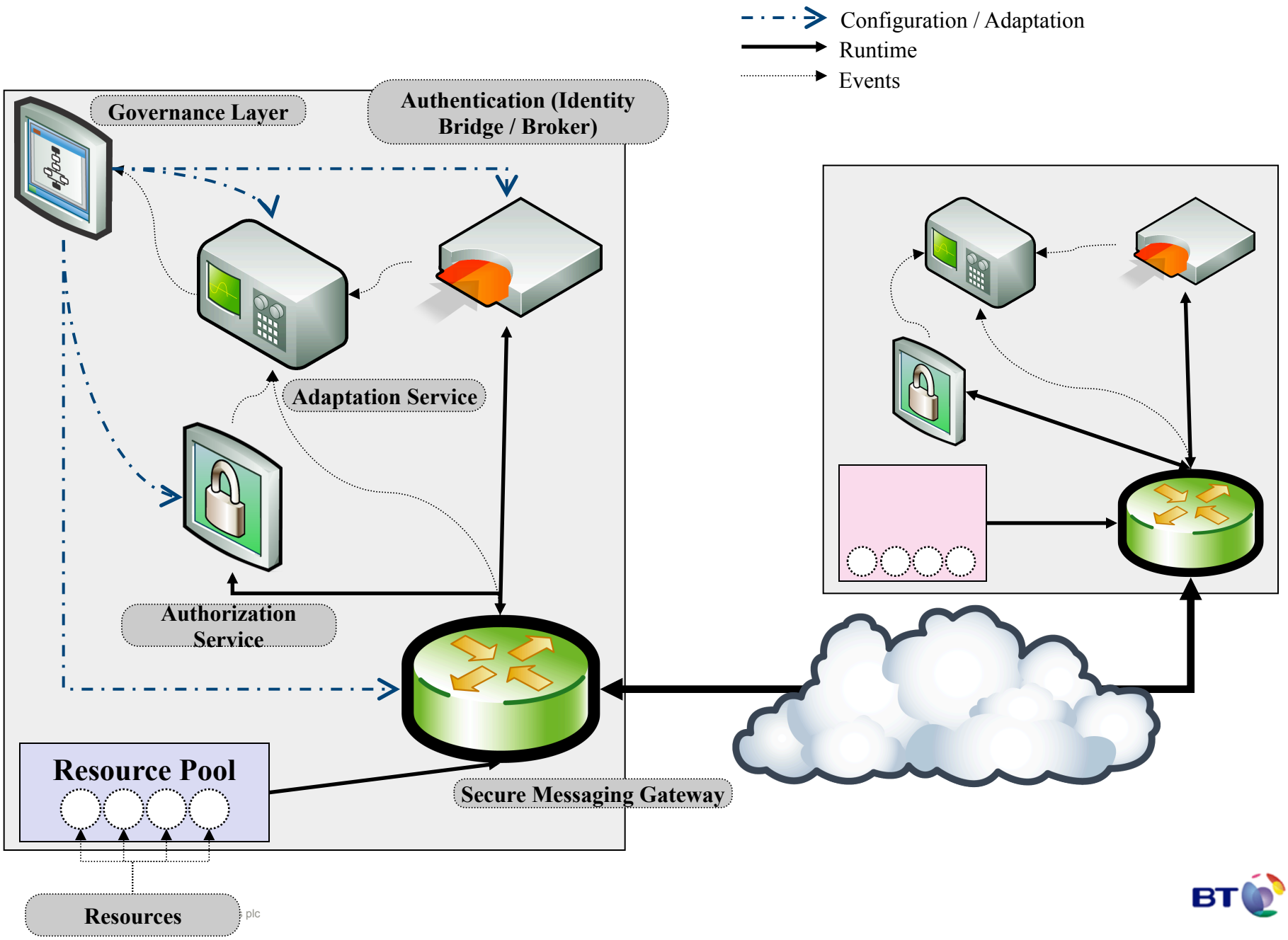
1. **infrastructure bindings – i.e. the enforcement and decision points used**
2. **policies about communication security, identity and access, monitoring and audit**
3. **the way that policies are evaluated and enforced**

change depending on both content & context of interactions

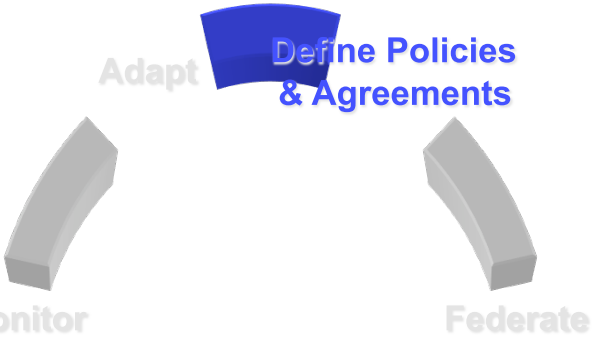
BT

BT Innovate's SON Security Approach

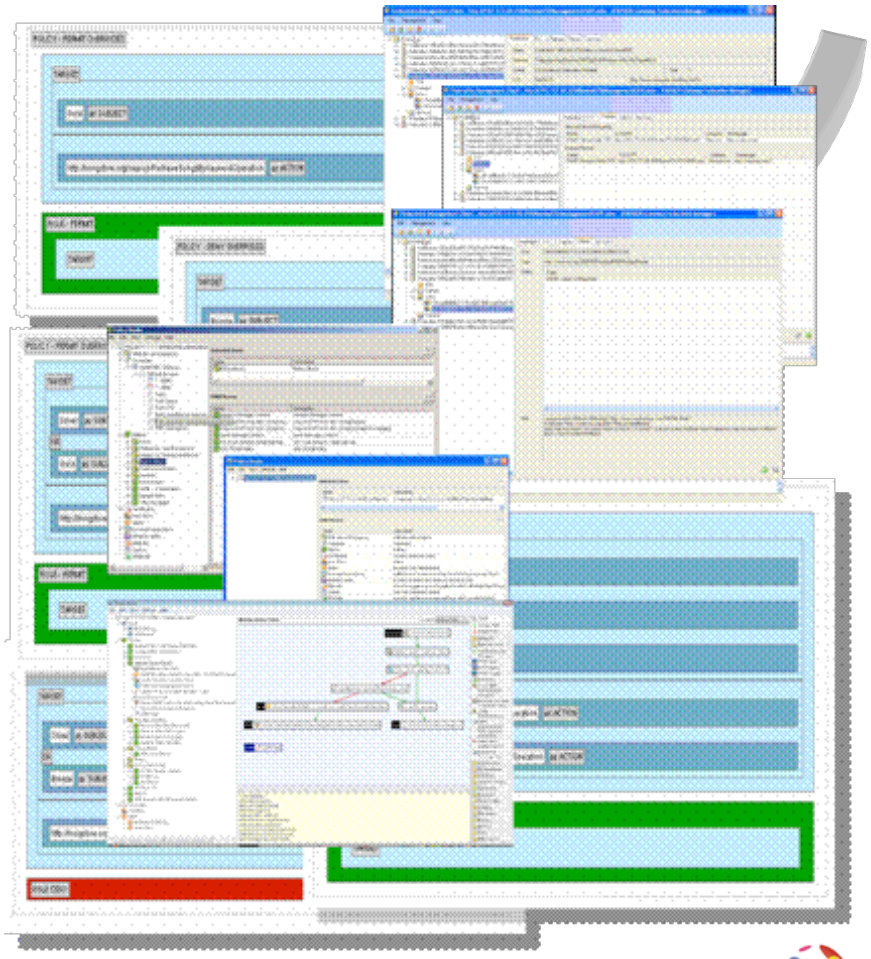



Configuration / Adaptation
Runtime
Events
Governance Layer
Authentication (Identity Bridge / Broker)
Adaptation Service
Authorization Service
Resource Pool
Secure Messaging Gateway
Resources

Define Policies & Agreements

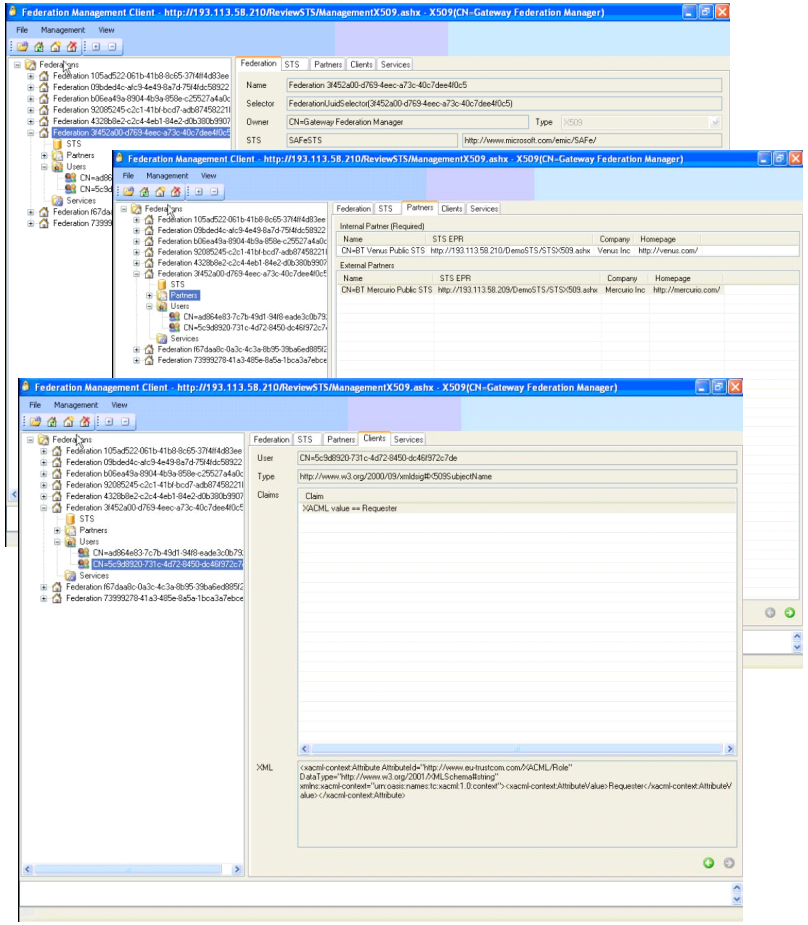


- Challenges
  - Coherent management of multiple services, domains, and administrators
  - Control the full policy-management life-cycle
  - Enable security outsourcing
- Innovation
  - Manages life-cycle of B2B collaborations capturing the key participants, their business functions, key interactions & the associated policies
  - Enables dynamic creation of services & contextualized exposure
  - Standards-based
  - High-level policy language



BT

Federate

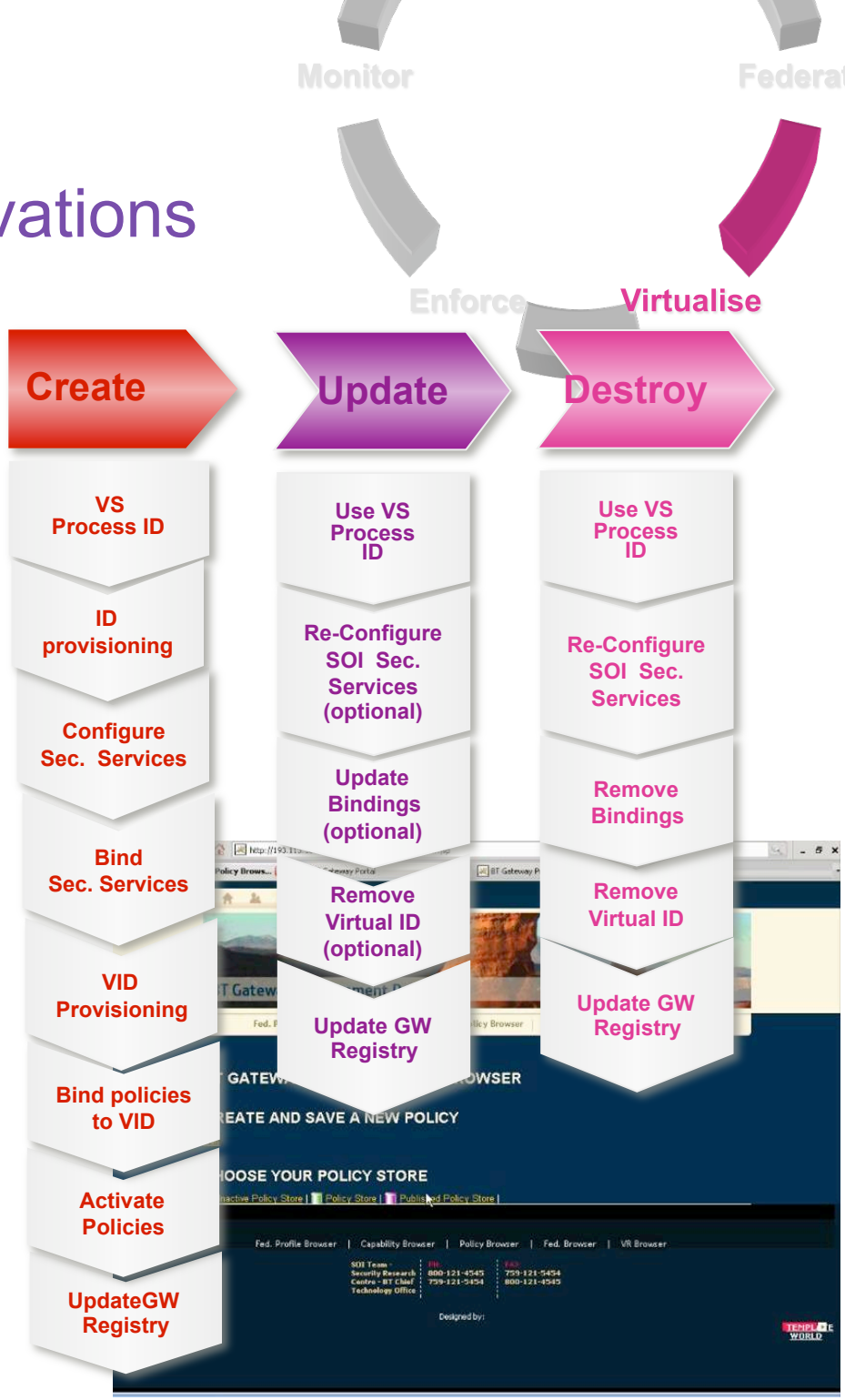


- Challenges
  - Context-based brokerage identities between heterogeneous systems
  - Manage multiple administrative authorities
  - Integrate 3rd party identity & attributes providers
- Innovation
  - Contextualized identity provisioning
  - Enable dynamic circle of trust establishment & dissymmetric trust relationships
  - Clear separation of administrative authorities

BT

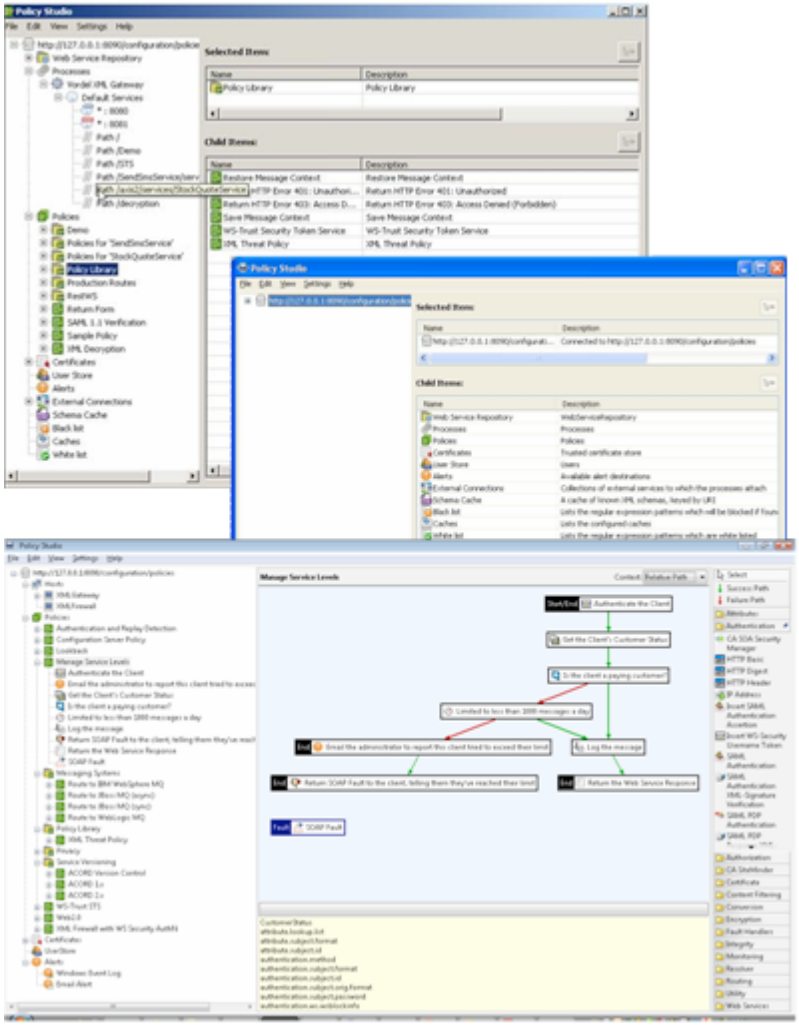
Key challenges and innovations

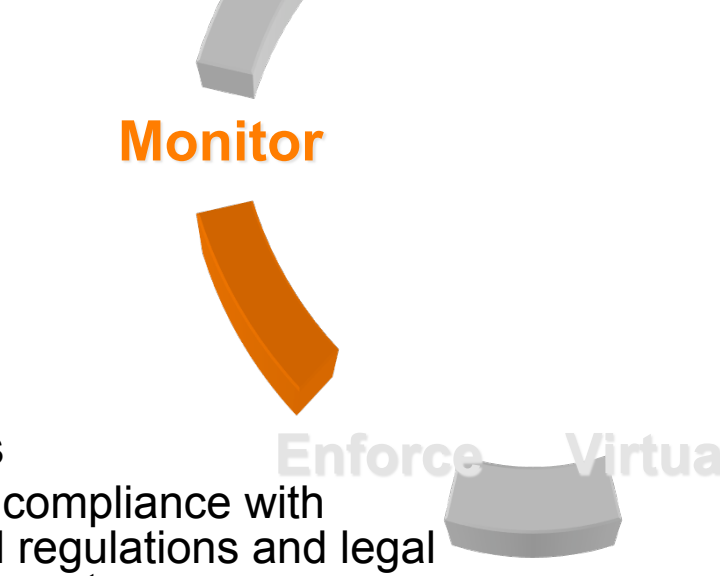
- Challenges
  - Define infrastructure profiles that include VAS security services & policy templates
  - Automate & secure service virtualization exposure
  - Control & monitor state of distributed infrastructure
- Innovation
  - Context-based binding of application instances to different polices and infrastructure
  - Contextualized virtual identity bindings to entitlements, privacy policies, resource utilisation…



Key challenges and innovations

- Challenges
  - Ensure data segregation and process isolation between unrelated E2E contexts
  - Threat protection in multiple layers
  - Mediation between identity realms
  - Policy-based, centralized enforcement
  - Enable Delegation of security requests to 3rd party services
- Innovation
  - Enterprise policy is enforced in the cloud
  - Contextualized enforcement isolating different service exposures
  - Security for Application networks: applications exposed as network-enabled services integrate over the network
  - Deperimeterisation: finely granular, content and context aware policies enforced at the E2E perimeter
  - Create the perception of disappearing boundaries



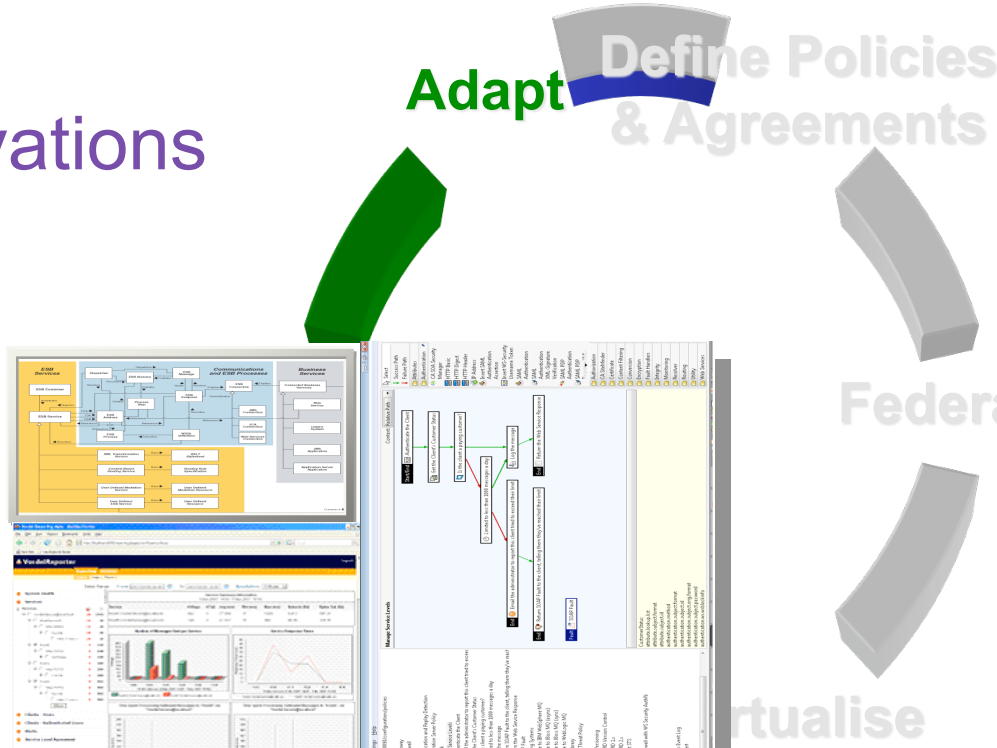


Key challenges and innovations

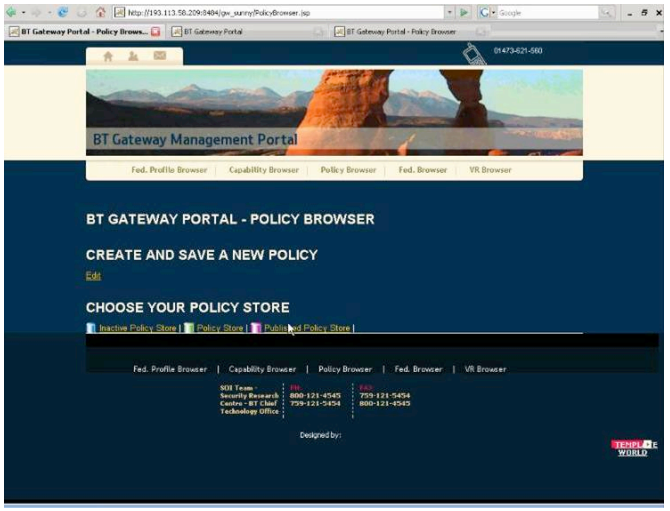
- Challenges
  - Assure compliance with internal regulations and legal requirements
  - Keep track of state evolution, policy versions, enable fallback scenarios
  - Provide full traceability
- Innovation
  - E2E security dashboard: privacy preserving security information sharing enables real-time monitoring of security state throughout the value chain
  - Granular Security Monitoring: policy refinement allows real-time security monitoring to identify violations of specific clauses of a security policy or an E2E agreement

BT

Key challenges and innovations



- Challenges
  - Adapt to changing conditions (environment, new threats) dynamically with zero downtime
  - Optimise performance, resource availability and business impact of security operations
  - Self-management
- Innovation
  - Improved Biz responsiveness.
  - Automatically determine the business impact of changes in the corporate structure, E2E transactions & resource availability
  - SOI that can react to changes.
  - Automatically adapt E2E operation based on the goals of E2E transactions and the context.



SOI Security – main common capabilities

- Configurable common security capabilities that have been designed to protect Web Services and Web 2.0 applications include the following:
  - **Secure message processing engine** allows protecting XML and Web Services messages in diverse transaction contexts. It can be virtualised to protect assets in different customer domains and clustered in order to support high-volume transactions
  - **B2B Federation services** allow managing the full life-cycle of circles of trust, identities and security attributes within and across enterprises
  - **Access Control services** allow distributed enforcement of access policies by multiple administrators, ensuring regulatory compliance, accountability and security audits
  - **Security Autonomics** allows reconfiguring the security services in response to security or QoS events in order to optimise performance, to respond to threats and to assure compliance with agreements and enterprise policies
  - **Policy Governance & life-cycle Management** allows to:
    - Expose enterprise resources and applications in different contexts using distinct virtualised security infrastructures per context
    - Manage the full life-cycle & dependencies of contextualised policies
- All security capabilities are exposed as web-services and can be managed remotely by means of standard Web Services management protocols

BT

Overall SON Gateways Benefits

Right First Time

- Differentiate policies & services used in collaborations
- Securely expose enterprise services in different collaboration contexts using multiple security providers
- Assess the correctness of security enforcement via the validation of declarative policies
- Regulatory compliance via policy coordination and auditability

Cycle Time

- Reduce the security management overhead
- Reduce integration timescales of value-adding security services
- Outsource the provisioning of VAS security services
- Exploit economies of scale by reusing a common security infrastructure in different collaboration contexts.

BT

Engagements with research & innovation partners

- Microsoft
  - Federation services designed and developed in collaboration with EMIC the European Microsoft Innovation Centre
  - Reviewed / adapted Microsoft's Web Service Security patterns
  - Joint work in TrustCoM R&D project resulted in amendments of WS-Federation and SAML profile for WS-Trust
- Atos Origin
  - Joint coordination of the TrustCoM and BEinGRID R&D projects
  - Joint pilots in the context of TrustCoM and BEinGRID R&D projects
  - Joint analysis of 25 business pilots in BEinGRID R&D project
- Vordel
  - Exploiting SOA gateways for Security Policy Enforcement
- Axiomatics AB & SICS
  - XACML3.0 compliant distributed authorisation service
  - Constrained delegation of administrative authority
- SAP Research
  - Working together of the B2B federation life-cycle management
- IBM Research
  - Security design patterns in collaboration with IBM Research in Zurich and NY USA

Examples & Exploitation

defence
home of the UK Ministry of Defence

- EU Collaborative Projects (BEinGRID,…)
- Defence
  - ESII: Strategic MoD projects in NATO countries for next generation Defence ICT infrastructure
  - DIF-DTC (General Dynamics UK-led research consortium)
- BT
  - SOI-SSG Security Research
  - Web 21C SDK
  - Policy life-cycle management capability
  - Ribbit
- Media market
  - Go! Messenger BT and Sony offering instant messaging VAS
  - BE09 – Online Gaming (as aforementioned)
- e-Health
  - Outsourcing of complex radiography processing for cancer patients
  - University hospital, supercomputing centre and local authorities in Spain

ESII
Enabling Secure Information Infrastructure

Sony PSP **Go!Messenger** Powered by BT
www.**gomessenger**.bt.com

BT and Ribbit

BT

Thank you!

For more info please contact us at theo.dimitrakos@bt.com or david.brossard@bt.com