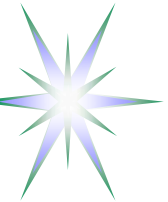
# Использование технологии Доверительной Компьютерной Платформы для повышения безопасности Виртуальной Рабочей Среды Грид

Yuri Demchenko <demch@science.uva.nl>
System and Network Engineering Group
University of Amsterdam

RELARN2007 Conference
6-9 June 2007, Nizhny Novgorod - Moscow, Russia



# Содержание

- Безопасность и доверие в Грид-приложениях
  - Отношения Пользователь-Провайдер и Данные-Компьютер
- Модель безопасной виртуальнй рабочей среды Грид
- Доверительная Компьютерная Платформа (ДКП) и Доверительный Платформенный Модуль (ДПМ)
- Выводы и дальнейшее развитие

# Безопасность и Доверие в Грид-приложениях и предоставлении контента

Виртуальная лаборатория (ВЛ/VL) как форма предоставления коммерческих услуг

- Фактически реализует концепцию Utility Computing
- Может ли провайдер ВЛ обеспечить доверительную среду для проведения экспериментов с точки зрения клиентов и бизнес-соперников
  - Эктремальный случай: Решится ли фирма *Pepsi выполнять свои анализы на оборудовании компании Coca-Cola?*
  - Здравый смысл: Мы можем доверять удаленной системе настолько насколько мы доверяем системному администратору

Провайдеры контента (музыка, видео)

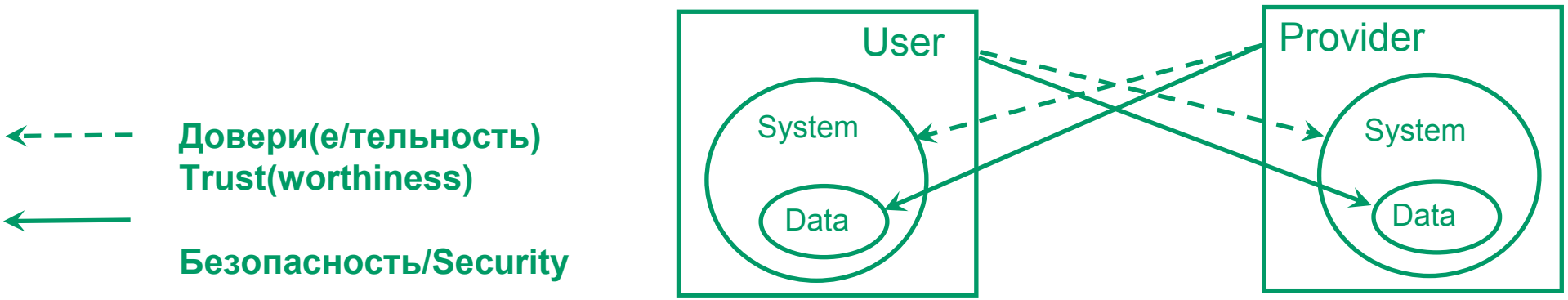
- Контент, который проигрывается на компьютере пользователя, должен быть защищен от копирования или использоваться такое количество, которое оплачено

Провайдеры сервисов/ресурсов по требованию (service on demand)

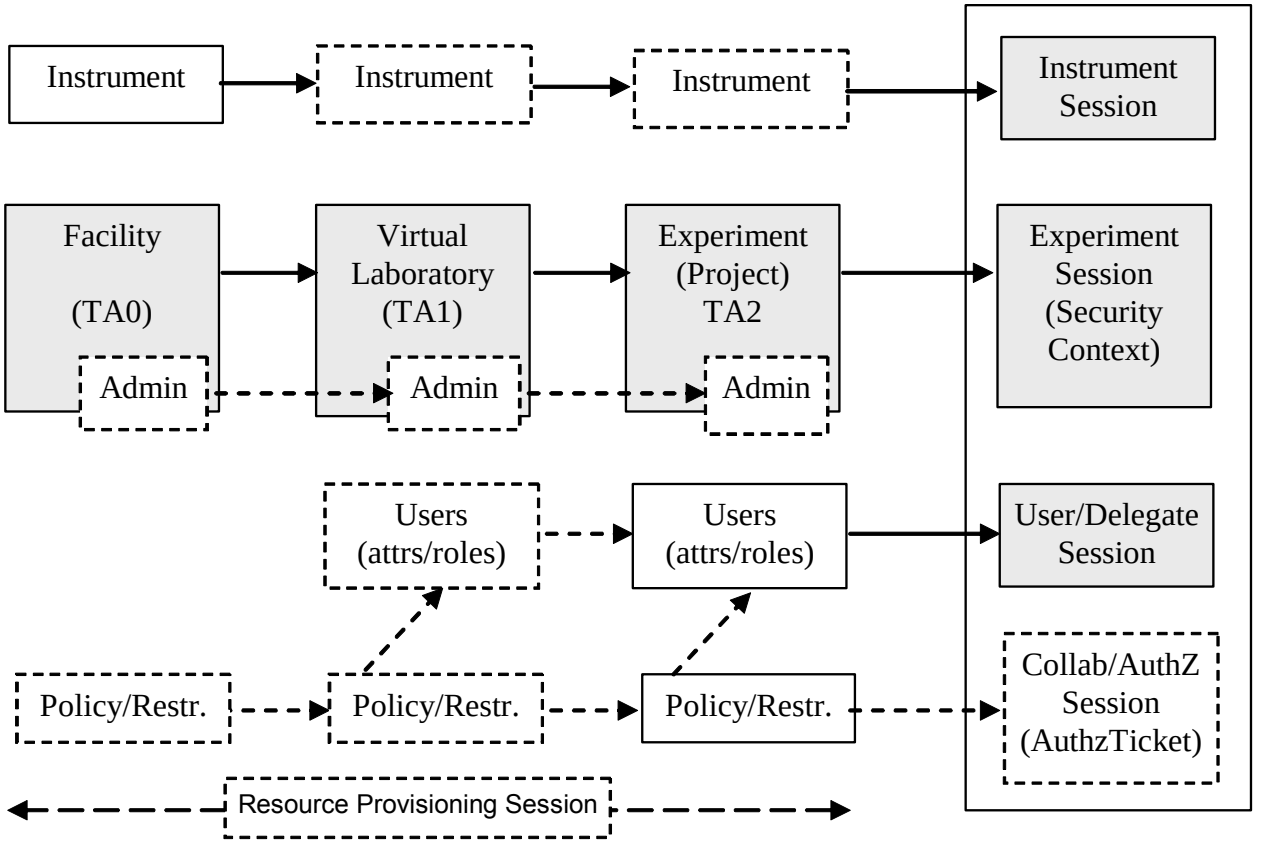
- Обеспечить выпольнение договора на предоставление услуг (SLA), включая «обьязательства» (Obligations), со стороны пользователя

# Разные стороны Безопасности и Доверия

- Современная реализация удаленных распределенных сервисов и цифрового контента делает отношения безопасности и доверительности между Пользователем и Провайдером более сложными
- Пользователь и Провайдер – 2 действующих лица, которые озабочены безопасностью и защищенностью собственных данных/контента и доверительностью компьютерных платформ друг друга
- Два аспекта безопасности и доверительности
  - Сохраненные данные и Обрабатываемые данные
  - Система выключенная и Система активная (обрабатывающая пользовательскую задачу/данные)
- Жизненный пример обеспечения специальной безопасности:
  - *Дипломатический визит или визит Президента*



# Доменная организация ресурсов в коллективной среде Виртуальной Лаборатории на основе Грид




- Динамическое создание рабочей среды эксперимента
- Создание динамических ассоциаций пользователей и ресурсов из множества доменов
- Использование договора ВЛ и/или Эксперимента для управления сеансами коллективной работы
- Обьединение политики безопасности множества доменов
- Возможность делегирования полномочий и прав в пределах ассоциации

Полное описание ресурса в форме URI/ID –

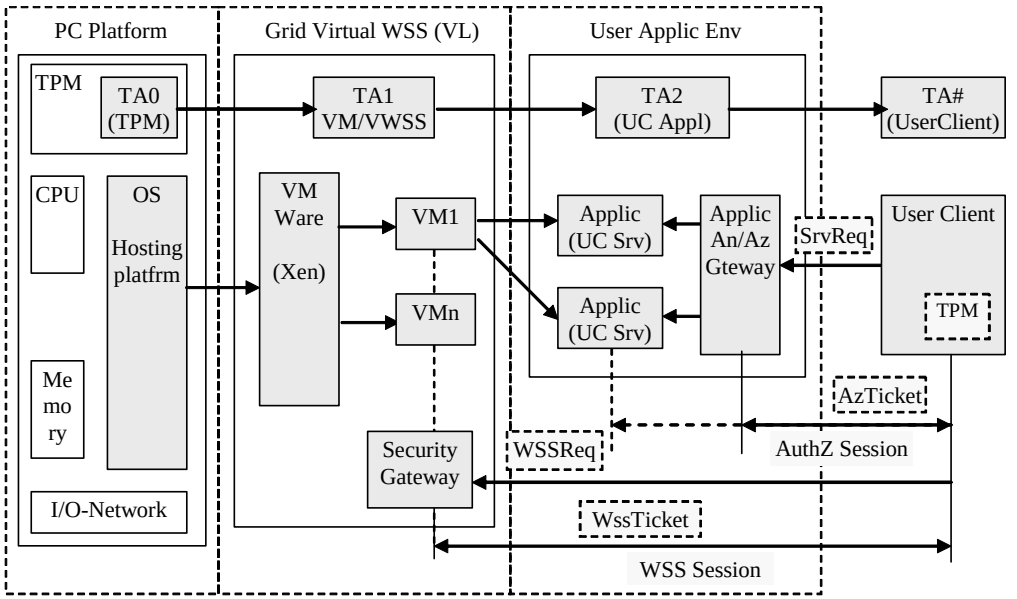
**CNL:Facility:VirtualLab:Experiment:InstrModel**

Полный контекст сеанса пользователя –

**Facility < Virtual Lab < Experiment < Experiment Session < Collaborative Session**

# Компоненты Доверительной среды Грид для Коллективных Приложений

- Доверительная компьютерная платформа (ДКП/TPM)
- Система виртуализации рабочего пространства (Virtual Workspace Service - VWSS)
- (Динамическая) система контроля доступа приложения




3-х уровневая безопасная пользовательская виртуальная среда

- User Controlled VWSS (VWSS-UC)

# Globus Toolkit Virtual Workspace Service (VWSS)

- Динамически конфигуримуемая исполнительная среда для динамических Грид-приложений - http://workspace.globus.org/index.html
  - Состоит из двух сервисов: Workspace Factory Service (WFS) и Workspace service (WSS)
  - Использует VM/Xen как платформу для виртуализации
- Предлагаемая модель безопасности использует только контроль доступа при запросе WFS на основе GT4-AuthZ
  - Возможность использования предварительно сконфигурированных образов VM
  - Использует доверие к провайдеру Грид-сервисов как к доверительной третьей стороне

# Доверительная Компьютерная платформа (ДКП)
# TCG Trusted Computing Platform

Предложена и развивается Trusted Computing Group (TCG)

- Предоставляет основу для построения контролируемой безопасной среды для исполнения задач и приложений и защищенной обработки данных или контента
  - https://www.trustedcomputinggroup.org/home
- Содержит стандарты для доверительного сетевого соединения, клиента, сервера, и мобильного устройства
- TMP software stack (TSS) определяет API/интерфейс для удаленного доступа, контроля идентификации платформы, PKI/СОК, безопасной e-mail, шифрование файлов и директорий, и др.

Компоненты TCG

- **Доверительный Платформенный Модуль (ДПМ, Trusted Platform Module (TPM))**
- “Curtained memory” в центральном процессорном устройстве
- Ядро безопасности в ОС и ядра безопасности в каждом приложении
- Поддерживающая инфраструктура онлайн серверов производителей аппаратного и программного обеспечения для производства, инсталяции и эксплуатации TPM/TCG

Trusted Network Connect (TNC) – позволяет производить контроль доверительных отношений и интегральности платформы при установлении соединения между двумя платформами с ДПМ

# Доверительный Платформенный Модудь (ДПМ)
# Trusted Platform Module (TPM)

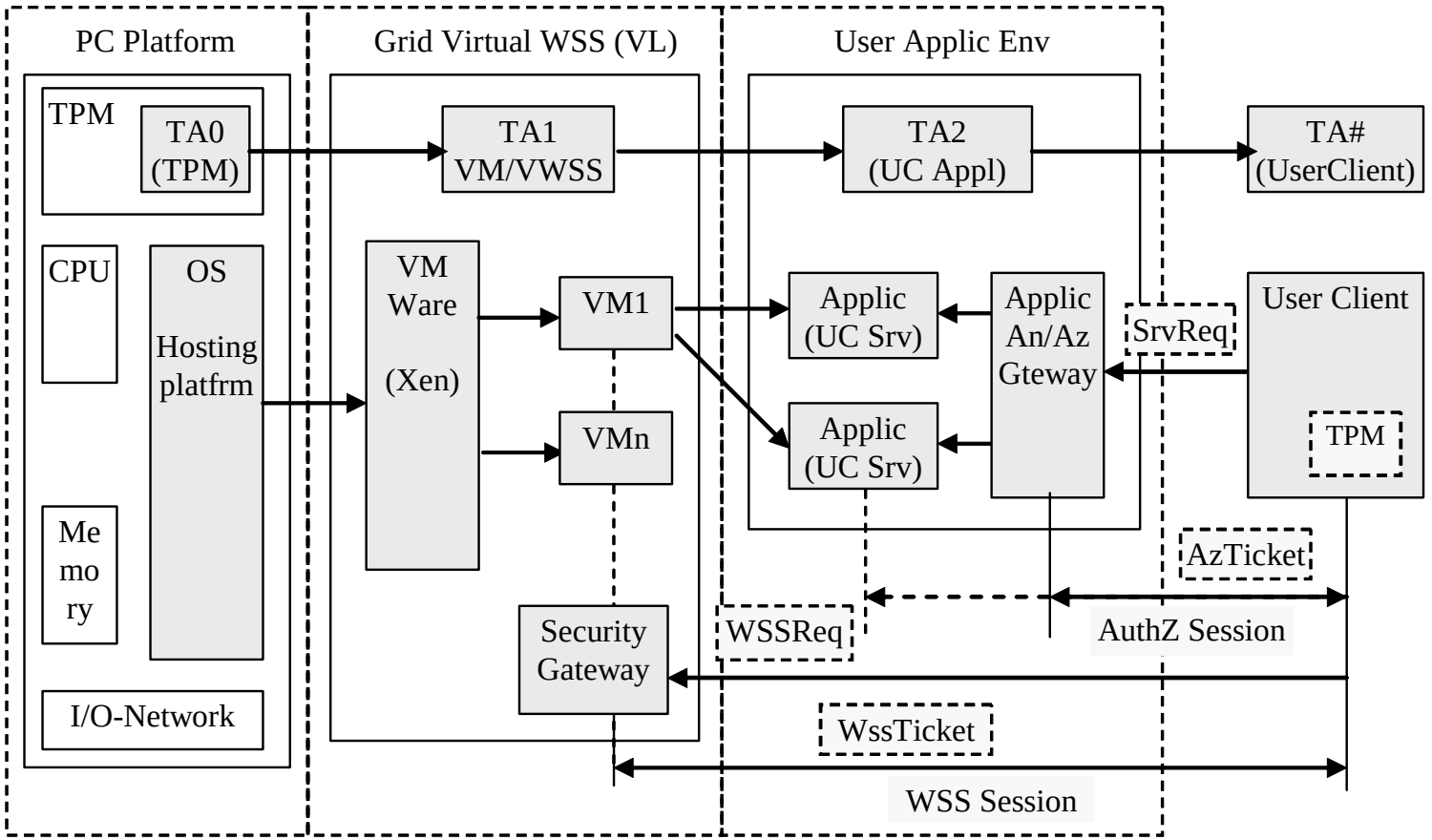
Микрочип, встроенный в компьютерную систему или пластиковую карточку

- Может использоваться как платформенная доверительная привязка (“root-of-trust”) для доверительной регистрации компьютерной системы и обеспечения ее интегральности

Обеспечивает набор аппаратно реализуемых криптографических функций

- Аппаратная генерация несимметричной пары ключей, аппаратная генерация цифровой подписи, шифрование посредством открытого или секретного ключа.
- Подтверждающий ключ (Endorsement Key (EK))
  - Реализует “zero-knowledge cryptography”
  - Позволяет доказать факт знания секретного ключа TPM без его раскрытия
- Протокол и процедура Прямой Автономной Аттестации (Direct Autonomous Attestation (DAA))
  - Позволяет безопасным образом передавать информацию о статической или динамической конфигурации платформы, которая может быть запомнена в TPM в хэшированной форме
- Защита коммуникаций между двумья TPM
- Монолитный счетчик и таймер, которые могут использоваться для контроля последовательности и временных параметров коммуникаций

# Безопасная пользовательская виртуальная среда – 3-х уровневая модель




- Trust Anchors: T0 (TPM) – TA1 (VM/VWSS) – TA2 (Application) – TA# (User)
- WVSS session and Application AuthZ sessions

# VWSS-UC – Соображения по внедрению

Компьютерная платформа содержащая TPM

- http://www.tonymcfadden.net/tpmvendors.html

Базовое программное обеспечение для TCG/TPM, разрабатываемое в рамках множества проектов

- Daonity (HP), OpenTC (EU), проекты в Germany, Czech Republic, инициативные исследования в проекте EGEE и UvA

Популярная среда виртуализации Xen v3.0 имеет так-называемый Virtual TPM модуль

- http://www.cl.cam.ac.uk/Research/SRG/netos/xen/readmes/user

Grid Virtual Workspace Service (VWSS) – GT4 candidate component

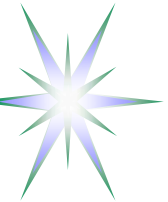
- http://workspace.globus.org/

Программный пакет GAAAPI для поддержки сеанса авторизации (Authorisation session)

- Использует квитанции авторизации (AuthZ Ticket) на основе XML или SAML

# Выводы и дальнейшее развитие

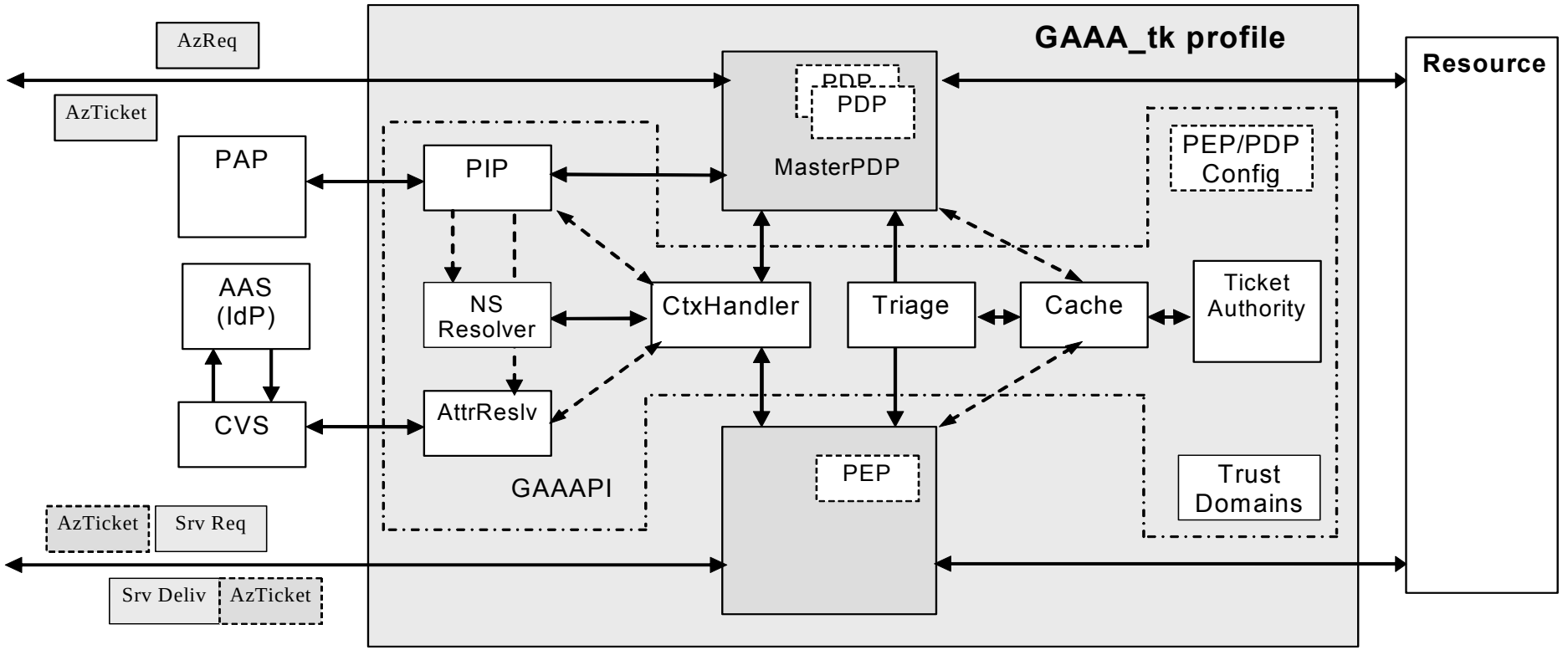
- TCG позволяет расширить зону доверительности для выполнения пользовательских задач и обработки данных
- Доверительная платформа может использоваться для исходного обмена доверительными сертификатами с целью последуюшего установления безопасного канала/среды между конечными системами Пользователя и Провайдера (aka end-to-end)
  - Предложена модель поддержки динамических ассоциаций на основе сеанса авторизации с использованием AuthZ Ticket
- Необходимо дальнейшее развитие и тестовое внедрение
  - Обсуждение в рамках OGF Virtualisation WG
- *Разработка модели управления динамическими отношениями доверительности для много-доменных виртуализованных ресурсов с TPM*



# Additional information

- AuthZ service components in GAAA-AuthZ and gJAF/GT4-AuthZ
- AuthZ session management and AuthZ ticket format

# GAAA-AuthZ/GAAAPI components to support dynamic security context management (1)

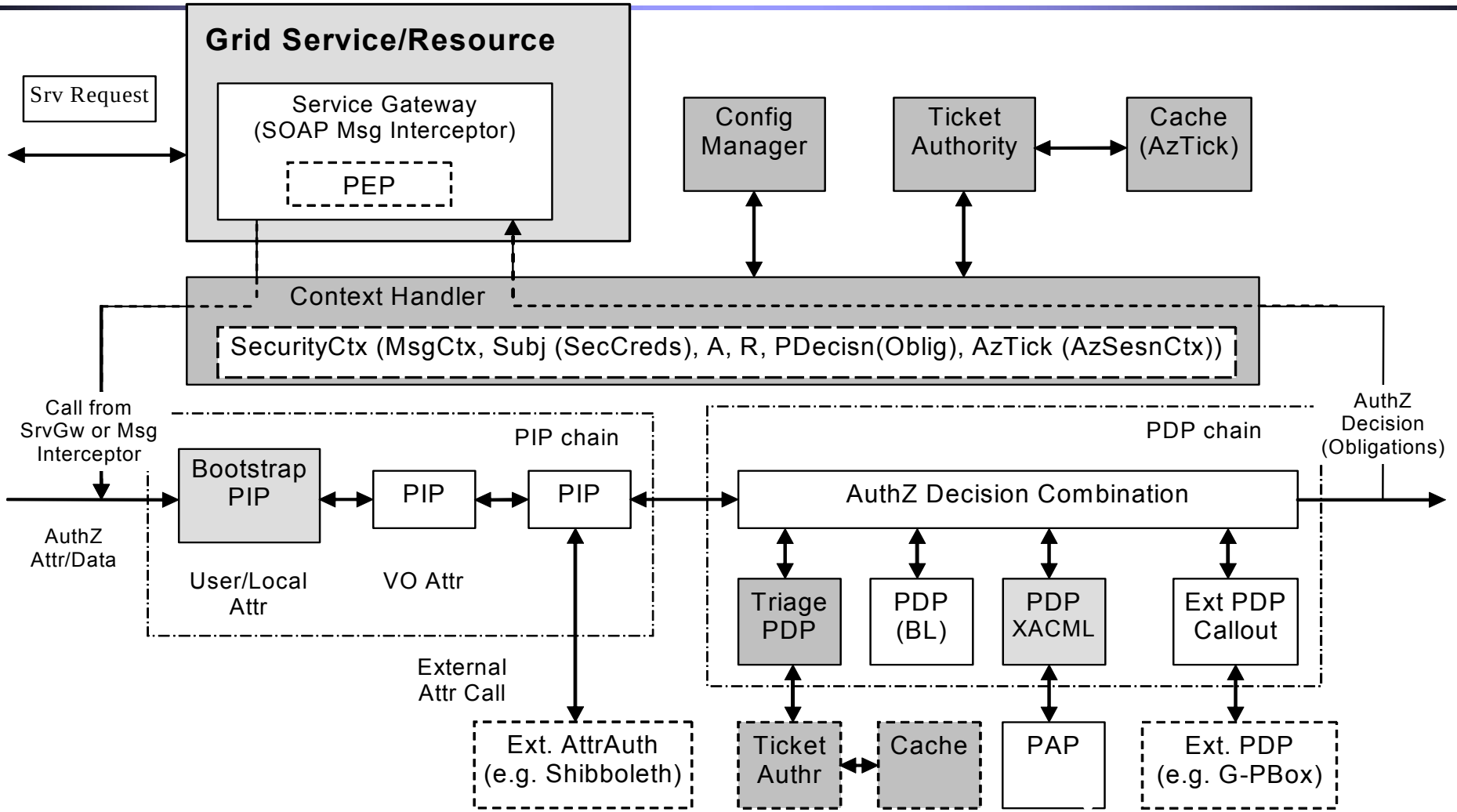



- GAAAPI is a collection of components to support PEP and PDP interaction, implemented in Java
- Needs Trust Anchor configuration in a distributed multidomain infrastructure

# GAAAPI components to support dynamic security context management (2)

- Context Handler (CtxHandler) that calls to a namespace resolver (NS Resolver) and attribute resolver (AttrResolver), which in its own can call to external CVS or Attribute Authority Service (AAS) *to validate* presented attributes or obtain new ones
- Triage and Cache to provide an initial evaluation of the request, including the validity of the provided credentials
  - Used for handling AuthZ tickets/tokens, and also for AuthZ session management by evaluating service requests versus the provided AuthZ ticket/token claims
- Ticket Authority (TickAuth) generates and validates AuthZ tickets or tokens on the requests from PEP or PDP
  - to support AuthZ session, tickets are cached by TickAuth directly or by PEP/PDP
- Policy Information Point (PIP) that provides resolution and call-outs to related authoritative Policy Authority Points (PAP)

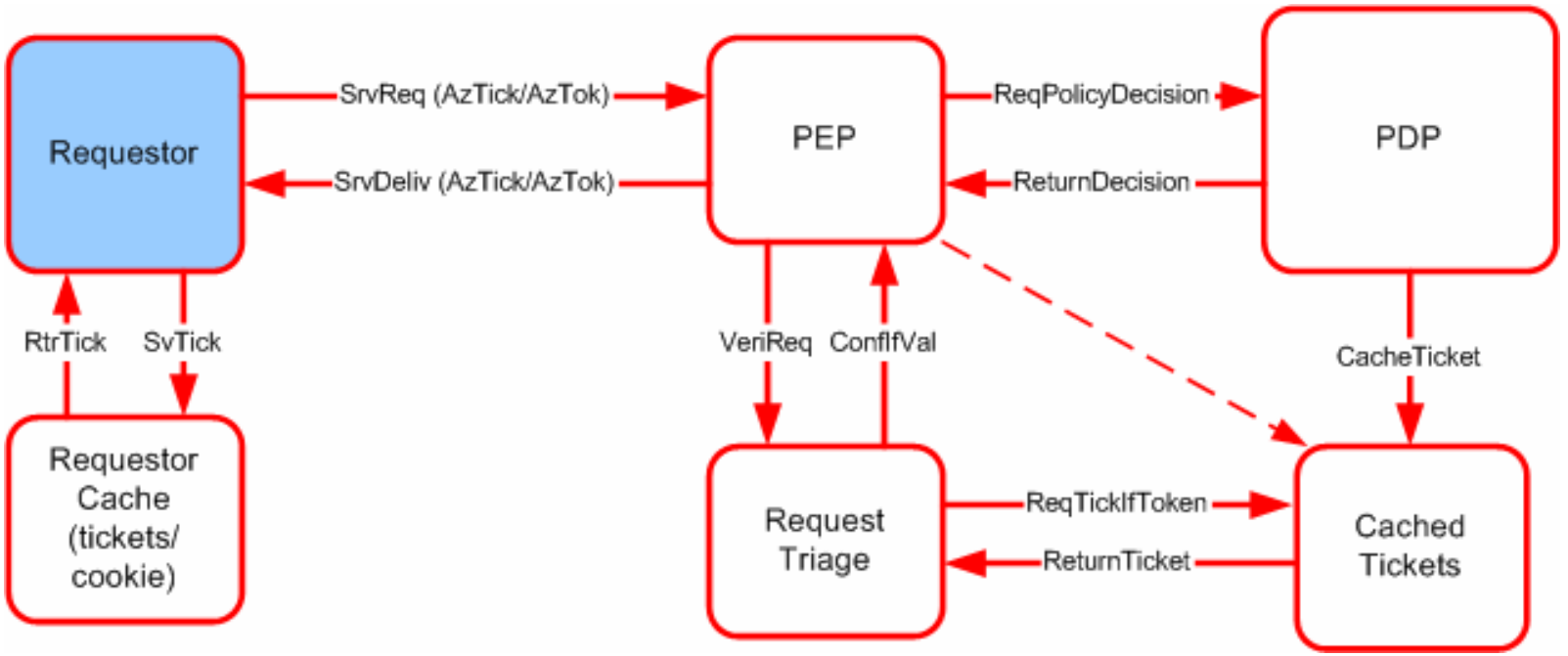
# gJAF – Proposed Extensions for AuthZ Session Management



# AuthZ Session management in GAAA-AuthZ

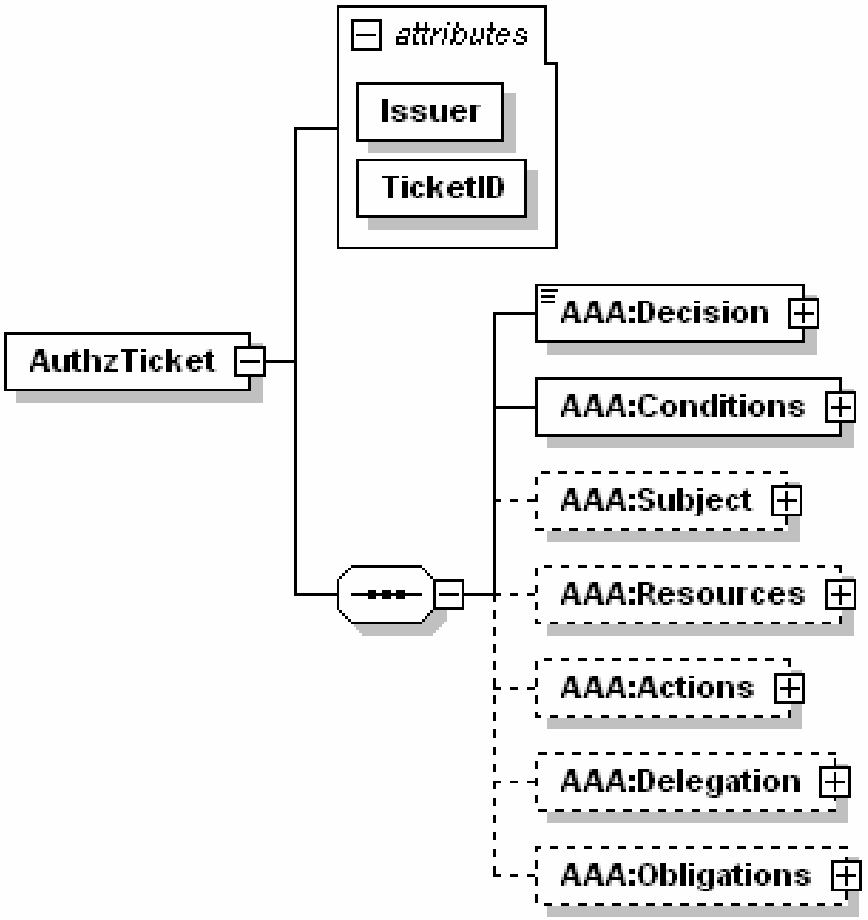
- AuthZ session is a part of the generic AAA-AuthZ functionality
- Session can be started only by an authorised Subject/Role
  - Session can be joined by other less privileged users
  - Session permissions/credentials can be delegated to (subordinate) subjects
- Session context includes Request/Decision information and may include any other environment or process data/information
  - AuthZ Session context is communicated in a form of extended AuthZ Assertion or AuthZ ticket
  - SessionID is included into AuthzTicket together with other AuthZ Ctx information
  - Signed AuthzTicket is cached by PEP (Policy Enforcement Point) or PDP (Policy Decision Point)
- If session is terminated, cached AuthzTicket is deleted
  - Note: AuthzTicket revocation should be done globally for the AuthZ trust domain

# AuthZ session Tickets/Tokens handling in AuthZ system



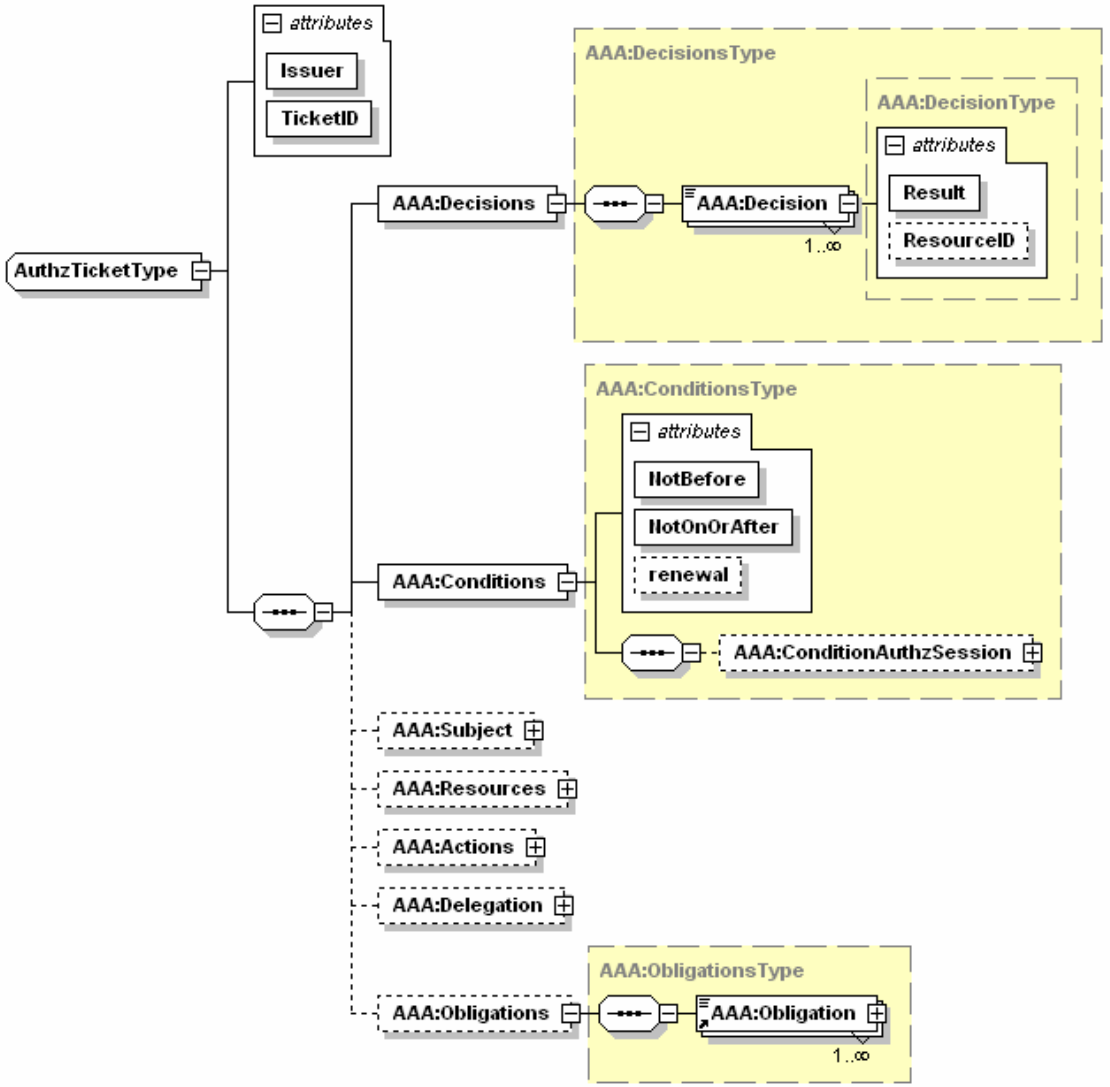

- AuthzTicket is issued by PDP and may be issued by PEP
- AuthzTicket must be signed
- AuthzTicket contains all necessary information to make local PEP-Triage Request verification
- When using AuthzTokens, AuthzTickets must be cached; Resolution mechanism from token to ticket must be provided

# AuthZ ticket/assertion for extended security context management – Data model (1) - Top elements



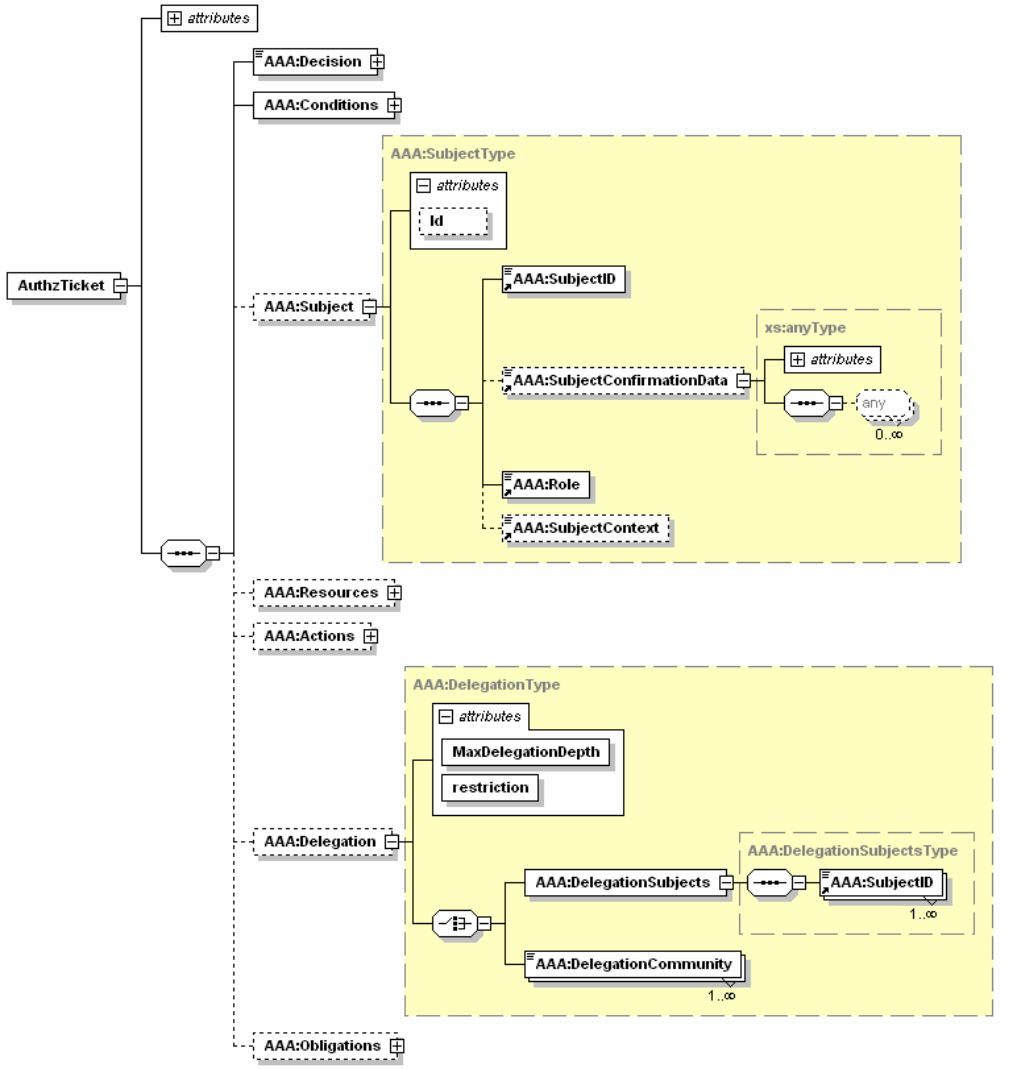

- Required functionality to support multidomain provisioning scenarios
  - Allows easy mapping to SAML and XACML related elements
- Allows multiple Attributes format (semantics, namespaces)
- Establish and maintain Trust relations between domains
  - Including Delegation
- Ensure Integrity of the AuthZ decision
  - Keeps AuthN/AuthZ context
  - Allow Obligated Decisions (e.g. XACML)
- Confidentiality
  - Creates a basis for user-controlled Secure session

# AuthZ ticket Data model (2) - Mandatory elements




- TicketID attribute
- Decisions element and ResourceID attribute
- Conditions Element and validity attributes
- Extensible element ConditionAuthzSession
  - Any AuthZ session related data

# AuthZ ticket Data model (3) – Subject and Delegation elements




- Subject element to keep AuthN security context and Subject Attributes
- Delegation element to allow permissions/AuthZ decision delegation to other Subjects or groups/community

# AuthZ ticket main elements

**<Decision>** element - holds the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute.

**<Conditions>** element - specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context

<ConditionAuthzSession> (extendable) - holds AuthZ session context

**<Subject>** complex element - contains all information related to the authenticated Subject who obtained permission to do the actions

<Role> - holds subject's capbilities

<SubjectConfirmationData> - typically holds AuthN context

<SubjectContext> (extendable) - provides additional security or session related information, e.g. Subject's VO, project, or federation.

**<Resources>/<Resource>** - contains resources list, access to which is granted by the ticket

**<Actions>/<Action>** complex element - contains actions which are permitted for the Subject or its delegates

**<Delegation>** element – defines who the permission and/or capability are delegated to: another DelegationSubjects or DelegationCommunity

- attributes define restriction on type and depth of delegation

**<Obligations>/<Obligation>** element - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.

# AuthZ ticket format (proprietary) for extended security context management – 3-10KB

```
<AAA:AuthzTicket xmlns:AAA="http://www.aaauthreach.org/ns/#AAA" Issuer="urn:cnl:trust:tickauth:pep"
    TicketID="cba06d1a9df148cf4200ef8f3e4fd2b3">
  <AAA:Decision ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</AAA:Decision>
    <!-- SAML mapping: <AuthorizationDecisionStatement Decision="*" Resource="*"> -->
  <AAA:Actions>
    <AAA:Action>cnl:actions:CtrlInstr</AAA:Action>     <!-- SAML mapping: <Action> -->
    <AAA:Action>cnl:actions:CtrlExper</AAA:Action>
  </AAA:Actions>
  <AAA:Subject Id="subject">
    <AAA:SubjectID>WHO740@users.collaboratory.nl</AAA:SubjectID>    <!-- SAML mapping: <Subject>/<NameIdentifier> -->
    <AAA:SubjectConfirmationData>IGhA11vwa8YQomTgB9Ege9JRNnld84AggaDkOb5WW4U=</AAA:SubjectConfirmationData>
    <!-- SAML mapping:  EXTENDED <SubjectConfirmationData/> -->
    <AAA:Role>analyst</AAA:Role>
    <!-- SAML mapping:  <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
    <AAA:SubjectContext>CNL2-XPS1-2005-02-02</AAA:SubjectContext>
    <!-- SAML mapping: <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue> -->
  </AAA:Subject>
  <AAA:Delegation MaxDelegationDepth="3" restriction="subjects">
    <!-- SAML mapping:  LIMITED <AudienceRestrictionCondition> (SAML1.1), or <ProxyRestriction>/<Audience> (SAML2.0)  -->
    <AAA:DelegationSubjects> <AAA:SubjectID>team-member-2</AAA:SubjectID> </AAA:DelegationSubjects>
  </AAA:Delegation>
  <AAA:Conditions NotBefore="2006-06-08T12:59:29.912Z" NotOnOrAfter="2006-06-09T12:59:29.912Z" renewal="no">
    <!-- SAML mapping: <Conditions NotBefore="*" NotOnOrAfter="*"> -->
    <AAA:ConditionAuthzSession PolicyRef="PolicyRef-GAAA-RBAC-test001" SessionID="JobXPS1-2006-001">
    <!-- SAML mapping: EXTENDED <SAMLConditionAuthzSession PolicyRef="*" SessionID="*"> -->
      <AAA:SessionData>put-session-data-Ctx-here</AAA:SessionData>  <!-- SAML EXTENDED: <SessionData/> -->
    </AAA:ConditionAuthzSession>
  </AAA:Conditions>
  <AAA:Obligations>
    <AAA:Obligation>put-policy-obligation(2)-here</AAA:Obligation>  <!-- SAML EXTENDED: <Advice>/<PolicyObligation> -->
    <AAA:Obligation>put-policy-obligation(1)-here</AAA:Obligation>
  </AAA:Obligations>
</AAA:AuthzTicket>
<ds:Signature> <ds:SignedInfo/> <ds:SignatureValue>e4E27kNwEXoVdnXIBpGVjpaBGVY71Nypos...</ds:SignatureValue></ds:Signature>
```

# AuthzToken example – 293 bytes

```
<AAA:AuthzToken TokenID="c24d2c7dba476041b7853e63689193ad">
<AAA:TokenValue>
0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKllWsq75IsHfusnm56
zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0sADm9If
X89Et55EkSE9oE9qBD8=
</AAA:TokenValue>
</AAA:AuthzToken>
```

AuthzToken is constructed of the AuthzTicket TicketID and SignatureValue

AuthzToken use suggests caching AuthzTicket's

AuthzToken can be used as cookie in Web/portal based applications