



Copyright © VBIC 2013  
All rights reserved

# Corporate Binding Rule Scheme (CBRS)

Cloud based inter/intra-organizational secure  
transfers of data across boundaries

*Prepared for*  
**VBIC**

**Version .1 Draft**

*Prepared by*

**Olaf Cames, MSc**  
.NET Security Advisor  
Azure Architectural Advisor  
[info@dotnetguru.net](mailto:info@dotnetguru.net)



VBIC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of VBIC.

VBIC may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from VBIC, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by VBIC. VBIC cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2014 VBIC. All rights reserved. Any use or distribution of these materials without express authorization of VBIC LLC is strictly prohibited.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

# Revision and Signoff Sheet

## Change Record

Date	Author	Version	Change reference
09/28/13	Olaf Cames	.1	Initial draft for review/discussion
			Release

# Table of Contents

## Contents

Executive summary.....	1
1. Internet Service Bus Orchestration .....	2
2. Enterprise Service Bus Pattern .....	3
3. AppFabric Service Bus and Access Control Service Bus Integration .....	4
4. Dedicated Service Bus Endpoints in corporate service namespace.....	5
5. Transport Client Credential Types .....	6
6. Enterprise wide Claims based Identity Management for Application & User .....	7
8. Enterprise wide Claims based Identity Management for non-SAML Applications	9
9. Minimum Procedure for external app interfacing.....	10
10. Standard Conversation - OOTB .....	11
11. Enterprise wide Claims based Identity Management for Application & User ....	12
12. Claims based Identity Management for User welcome but just optional .....	13
13. Minimum security procedure for external app interfacing .....	14
14. Minimum security procedure for external app interfacing .....	15
15. Application Normative Framework (PoC candidates) .....	16
16. Evidence that information being used or stored by applications is adequately protected .....	17
17. Corporate Binding Rule Scheme (CBRS) .....	18

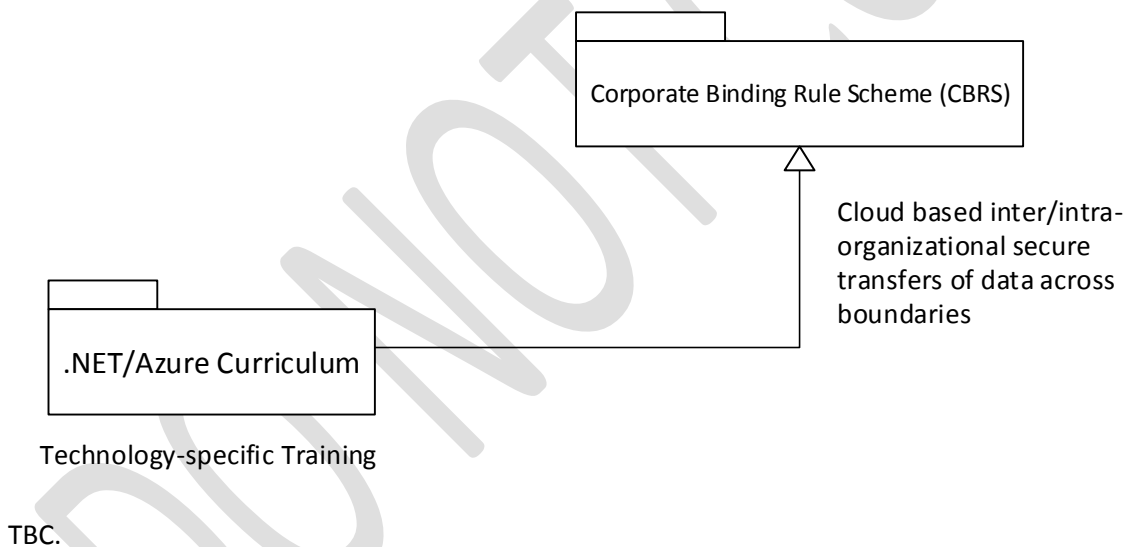
## Executive summary

The requirements and processes specified in this draft status document are not intended to be implemented in isolation but rather integrated into existing processes. To this effect, Azure implementer should map their existing processes and frameworks to those proposed by .NET/Azure application security, thus reducing the impact of implementing .NET application security.

.NET/Azure application security is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

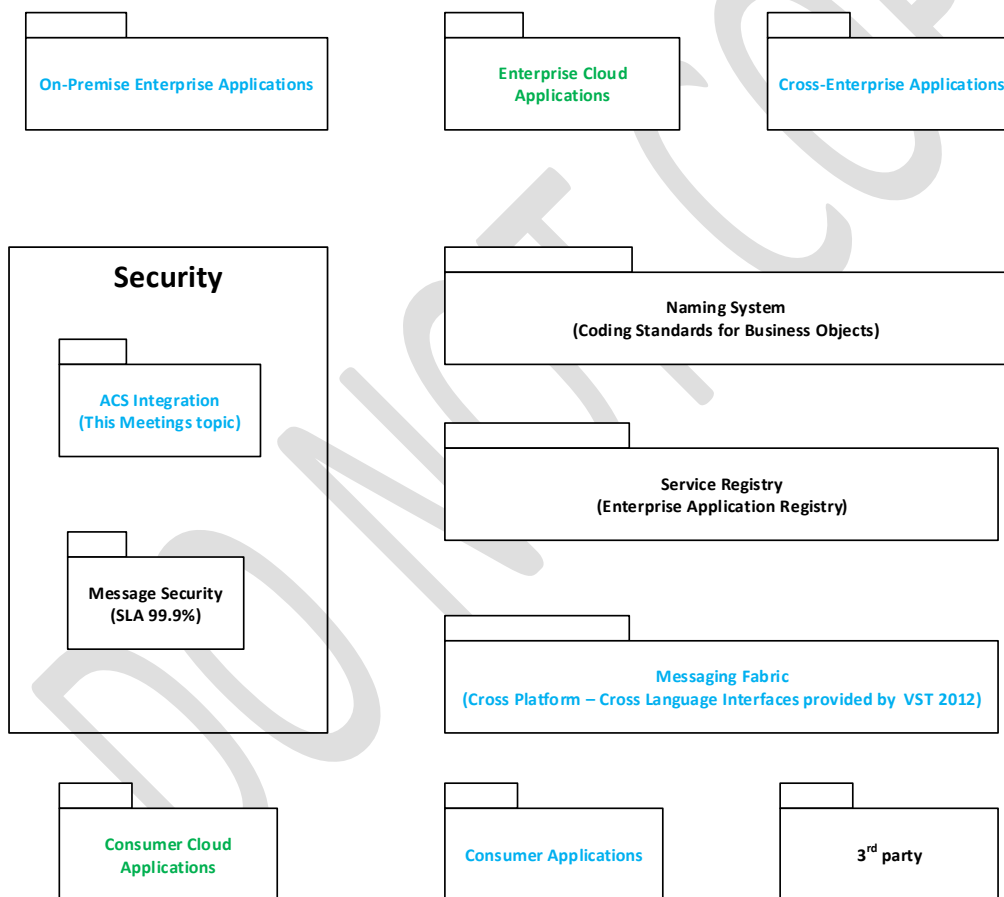
This documents hosts diagrams intended to visualize the Application Security Controls used on a hypothetical use cases, usage scenarios and PoC projects. Many teams will/can/should add other security and privacy tasks that are specific to their projects.

Relationship to other documents (release date schedule ~ TBD)



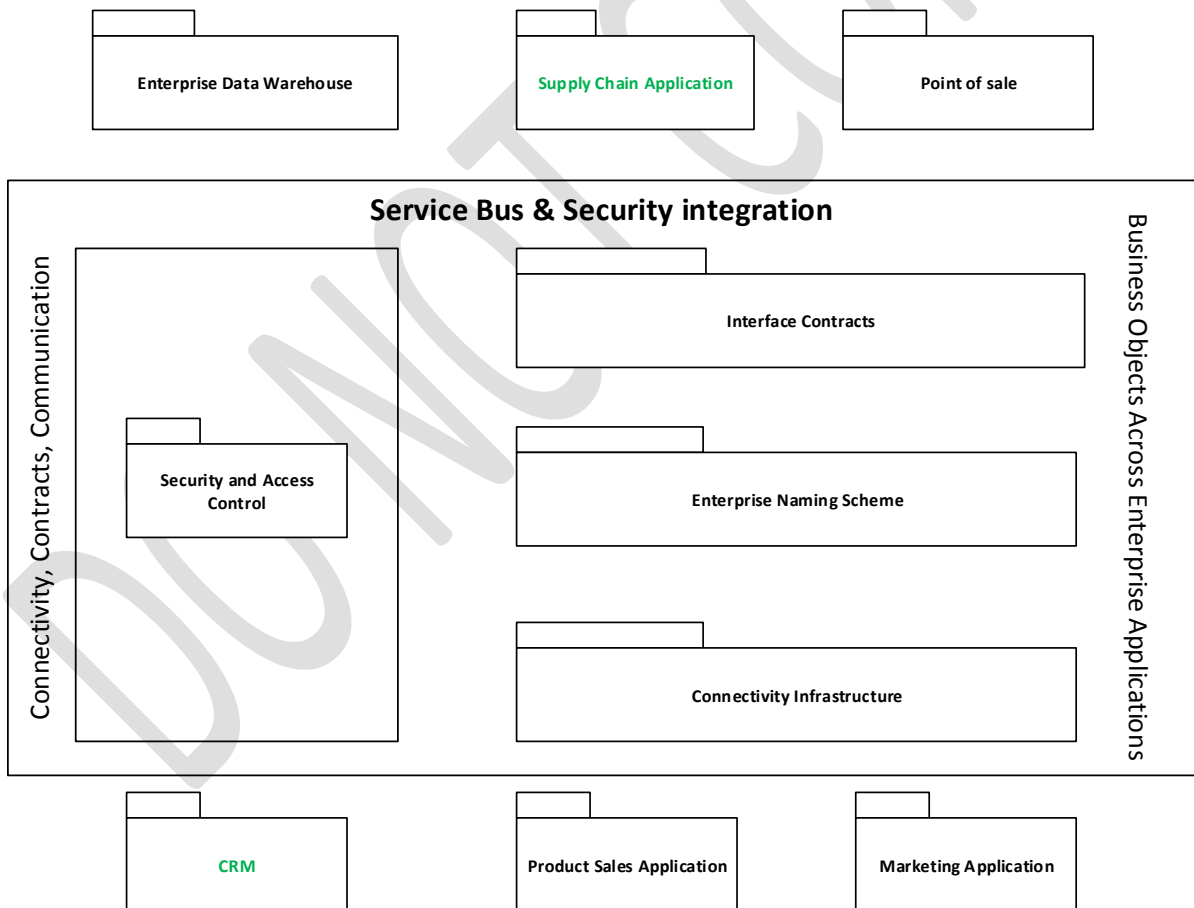
## 1. Internet Service Bus Orchestration

# Internet Service Bus Orchestration



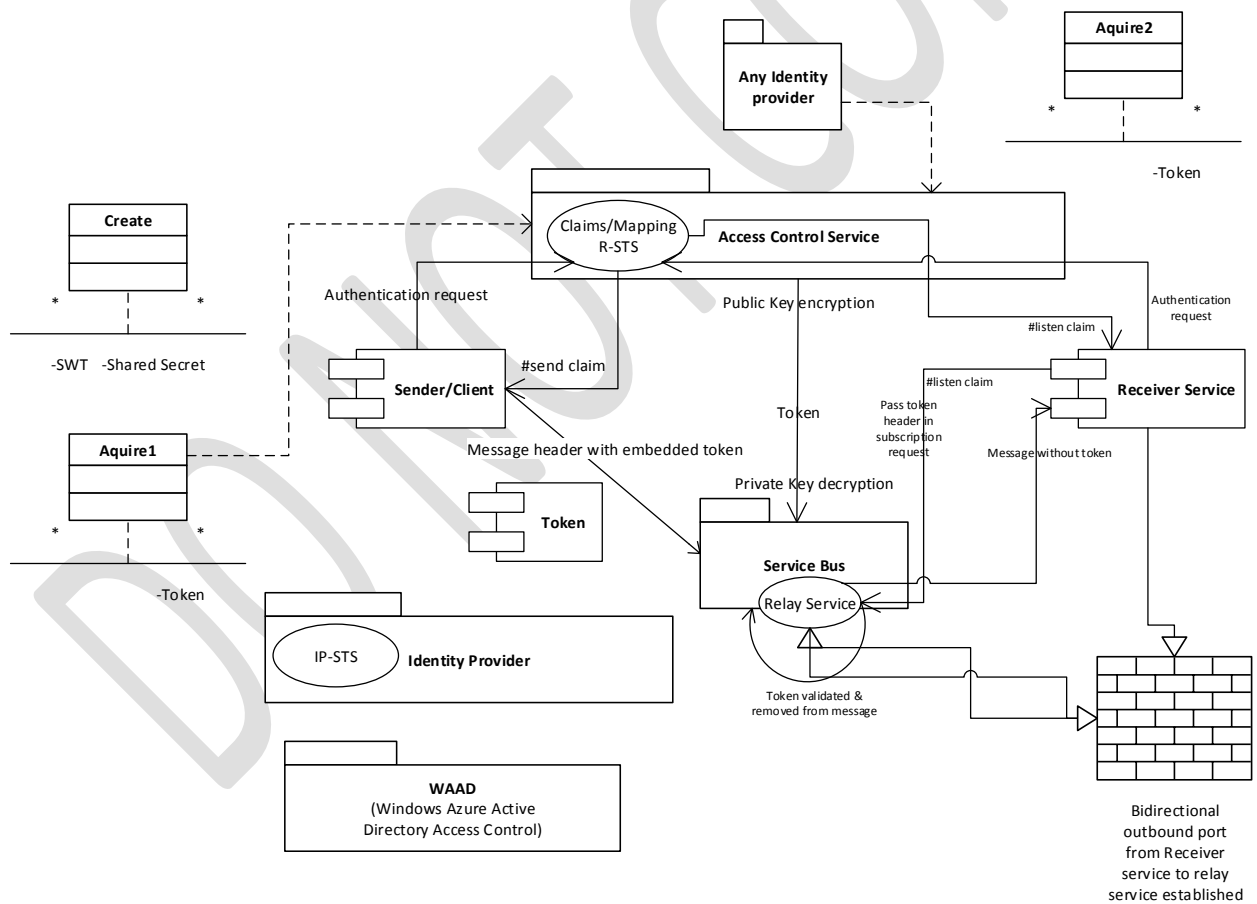
## 2. Enterprise Service Bus Pattern

# Enterprise Service Bus Pattern



### 3. AppFabric Service Bus and Access Control Service Bus Integration

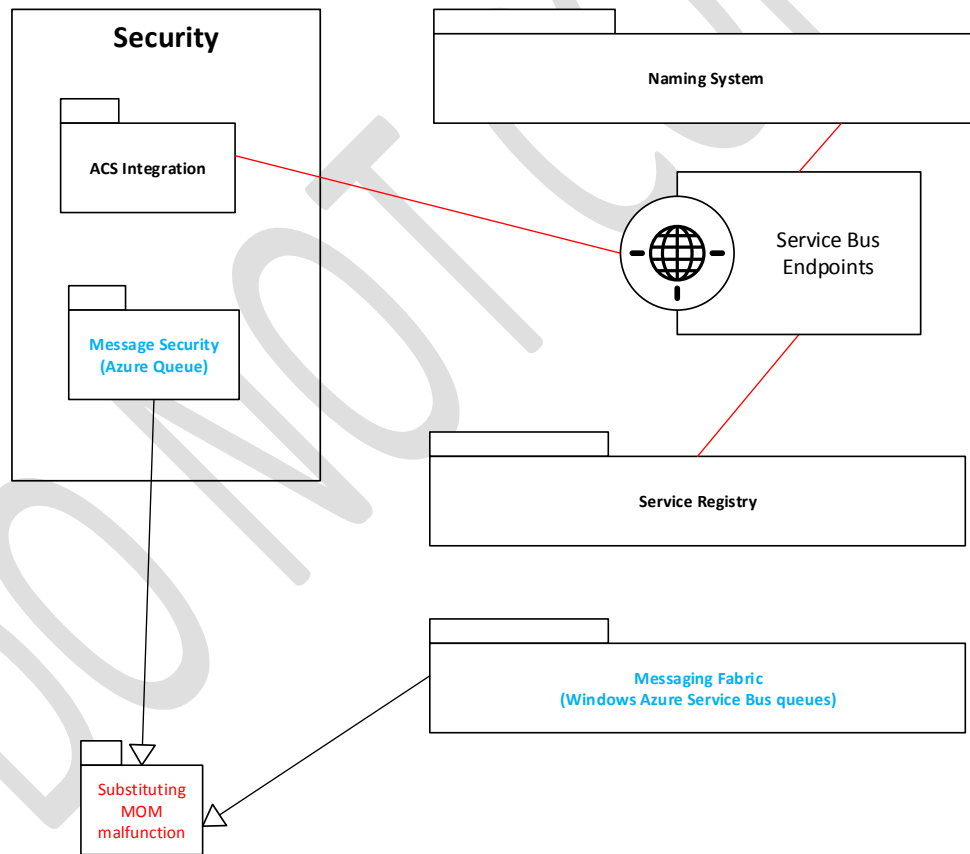
## AppFabric Service Bus and Access Control Service Bus Integration





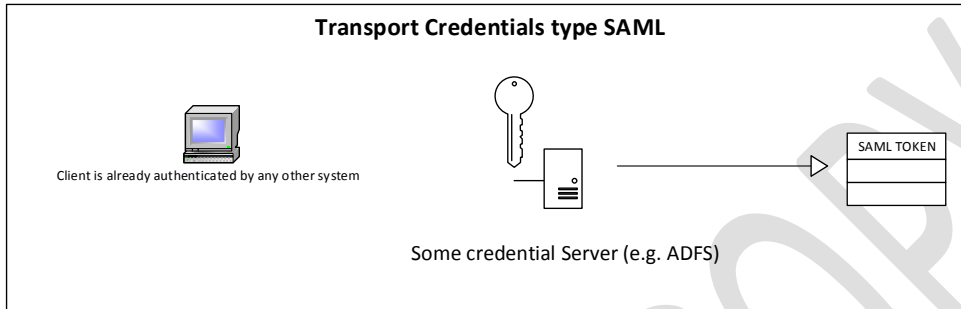
## 4. Dedicated Service Bus Endpoints in corporate service namespace

ACS creates dedicated Service Bus endpoints in your service namespace

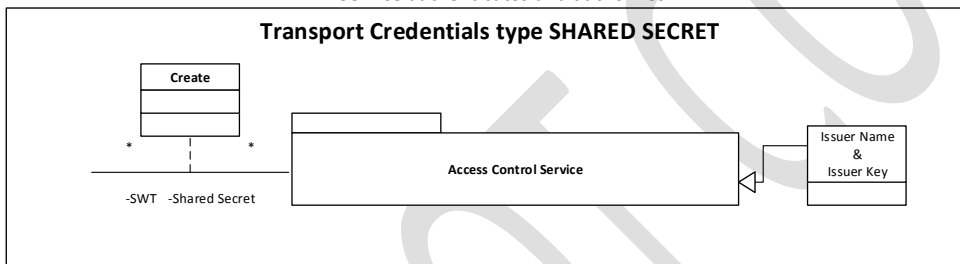


## 5. Transport Client Credential Types

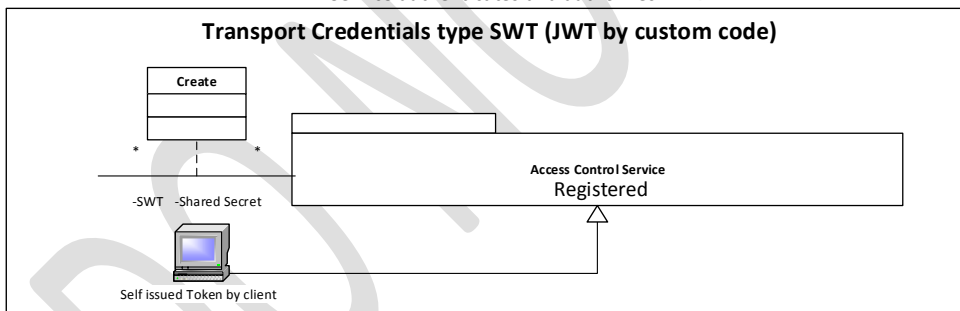
### Transport Client Credential Types



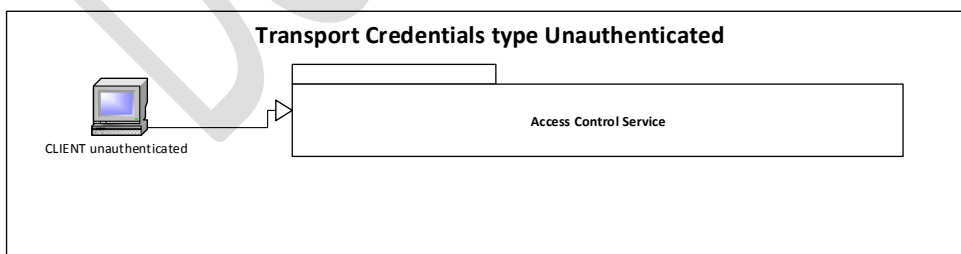
Service authenticates and authorizes



Service authenticates and authorizes



Service does not authenticate and authorize

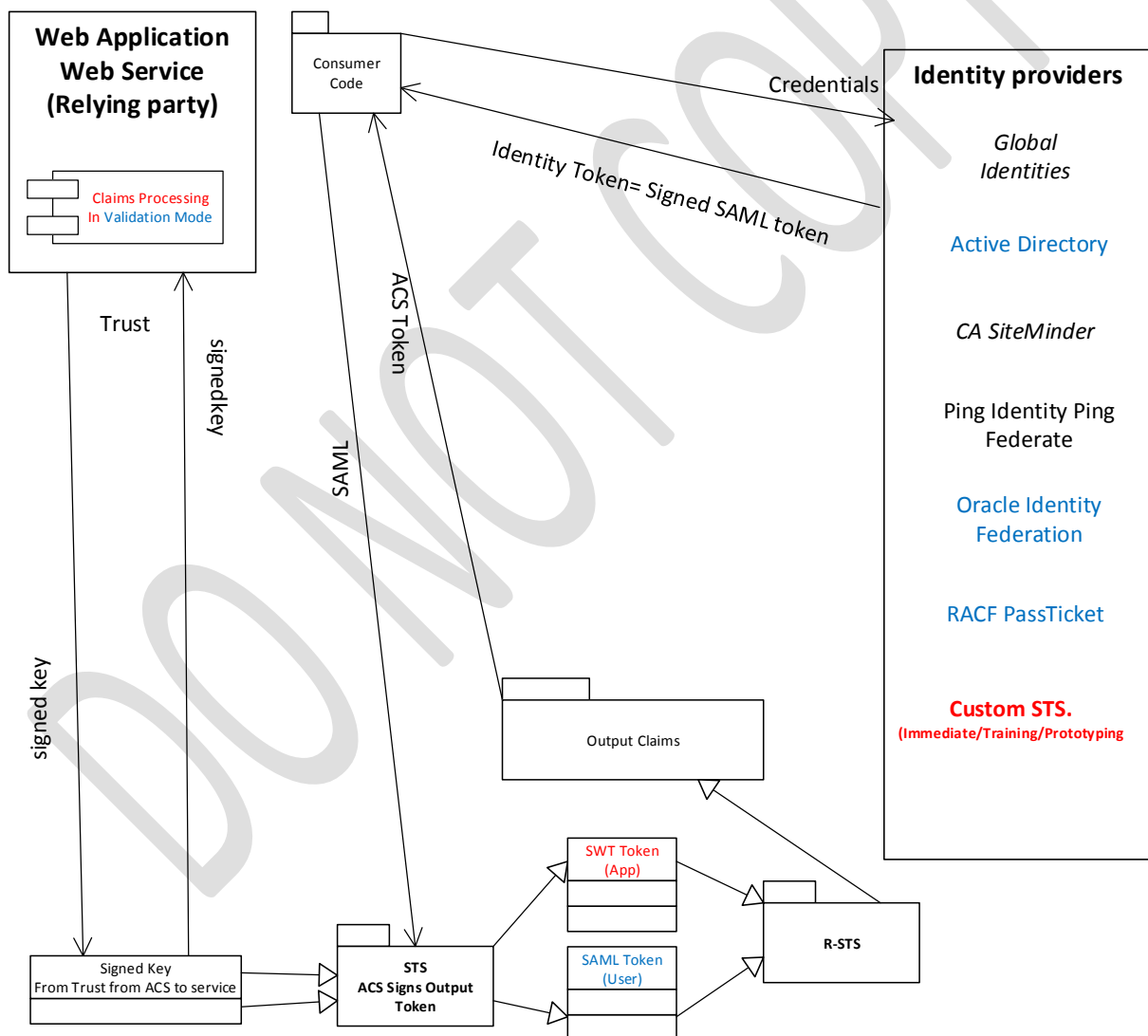


Service authenticates and authorizes

## 6. Enterprise wide Claims based Identity Management for Application & User

### Enterprise wide Claims based Identity Management for Application & User

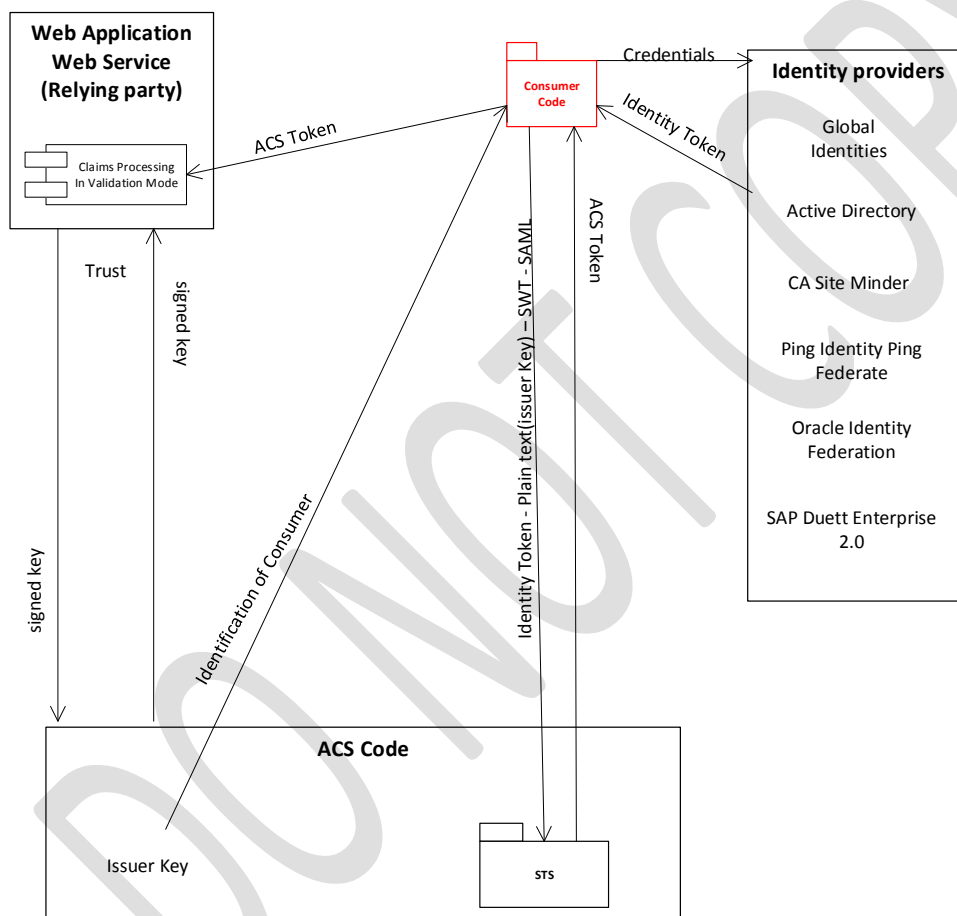
(High performance in Azure provided – Current Infrastructure too weak)



## 7. Enterprise wide Claims based Identity Management for Applications

### Enterprise wide Claims based Identity Management for Application

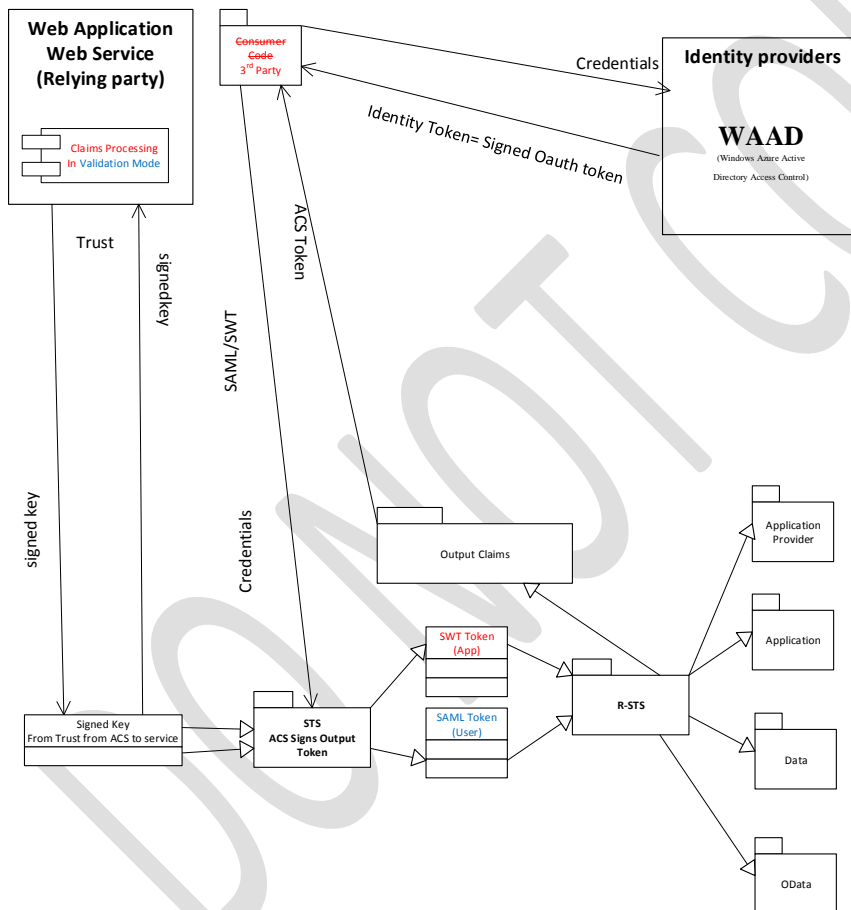
(Claims based Identity Management for user welcome but just optional)



## 8. Enterprise wide Claims based Identity Management for non-SAML Applications

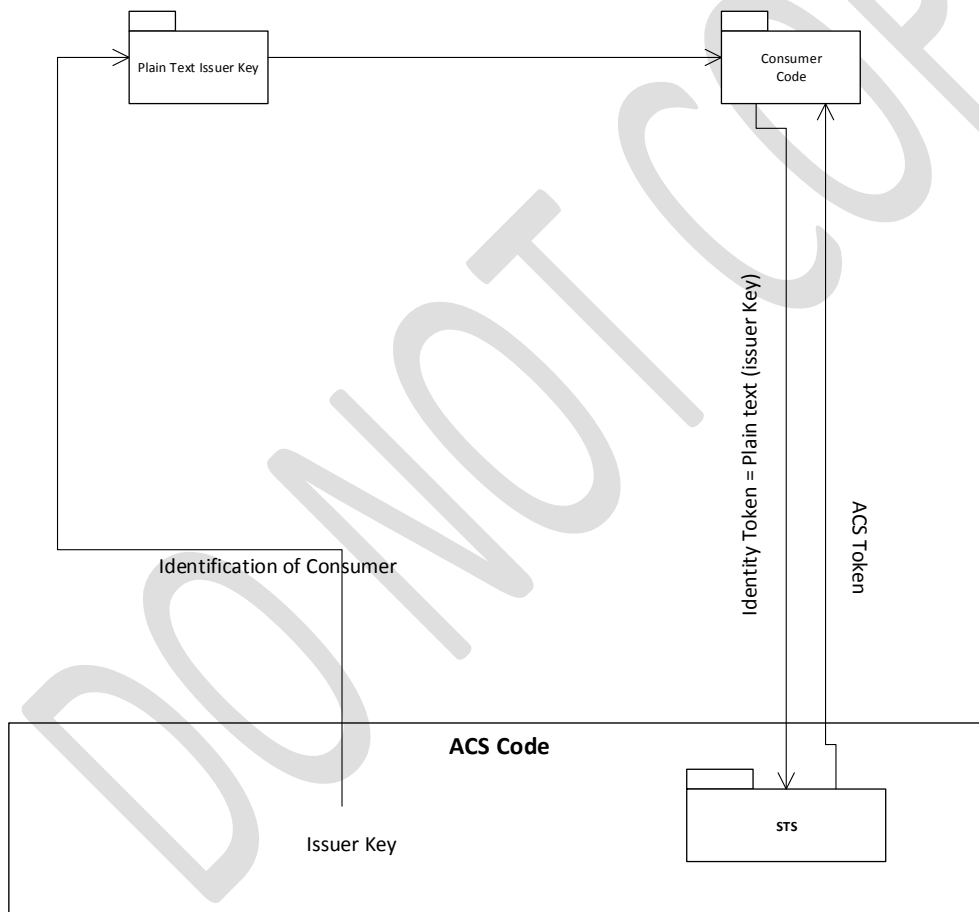
### Enterprise wide Claims based Identity Management for non-SAML Applications

(High performance in Azure provided – Current Infrastructure too weak)



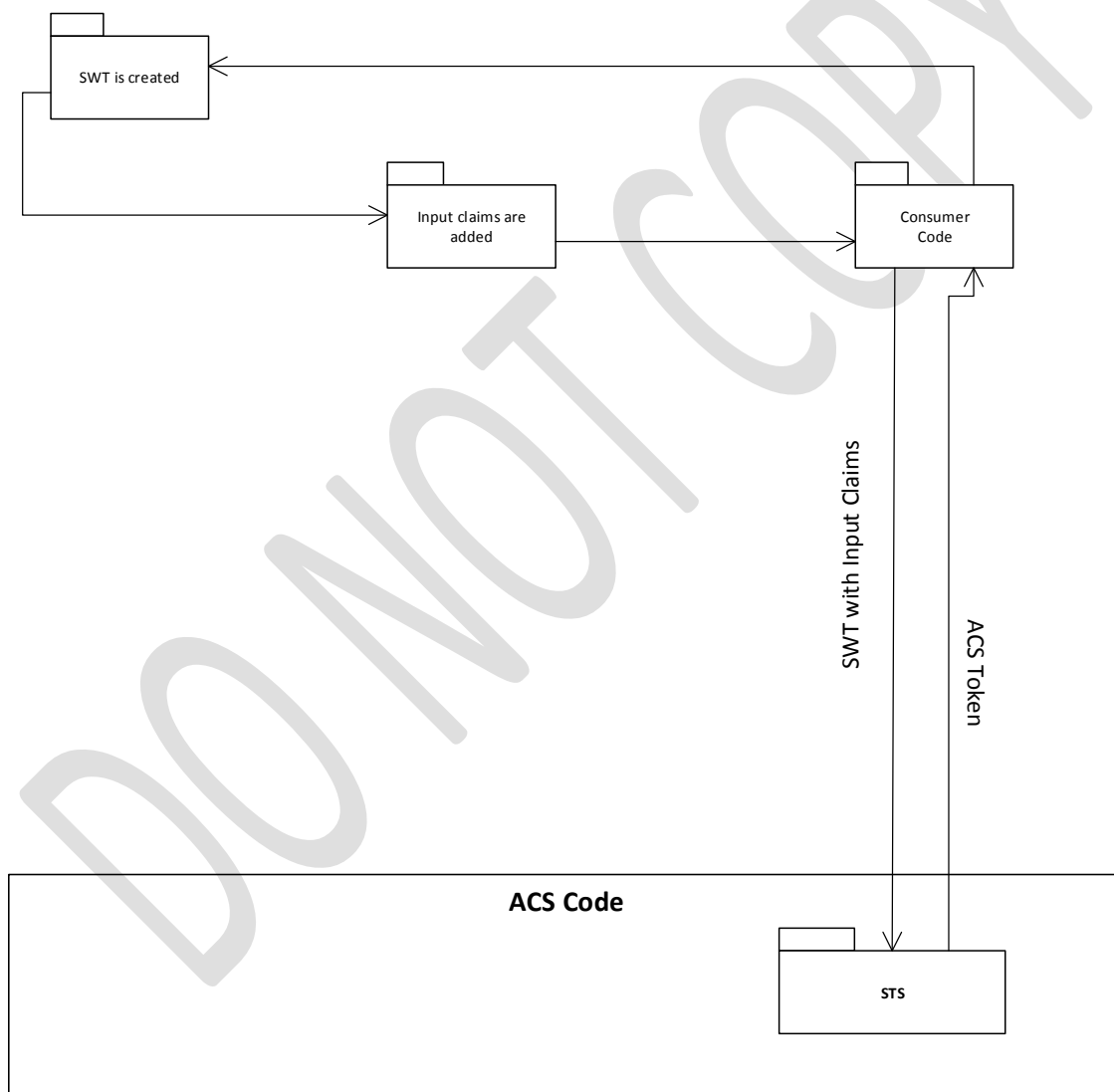
## 9. Minimum Procedure for external app interfacing

### Enterprise wide Claims based Identity Management for Application (Minimum procedure for external app interfacing)



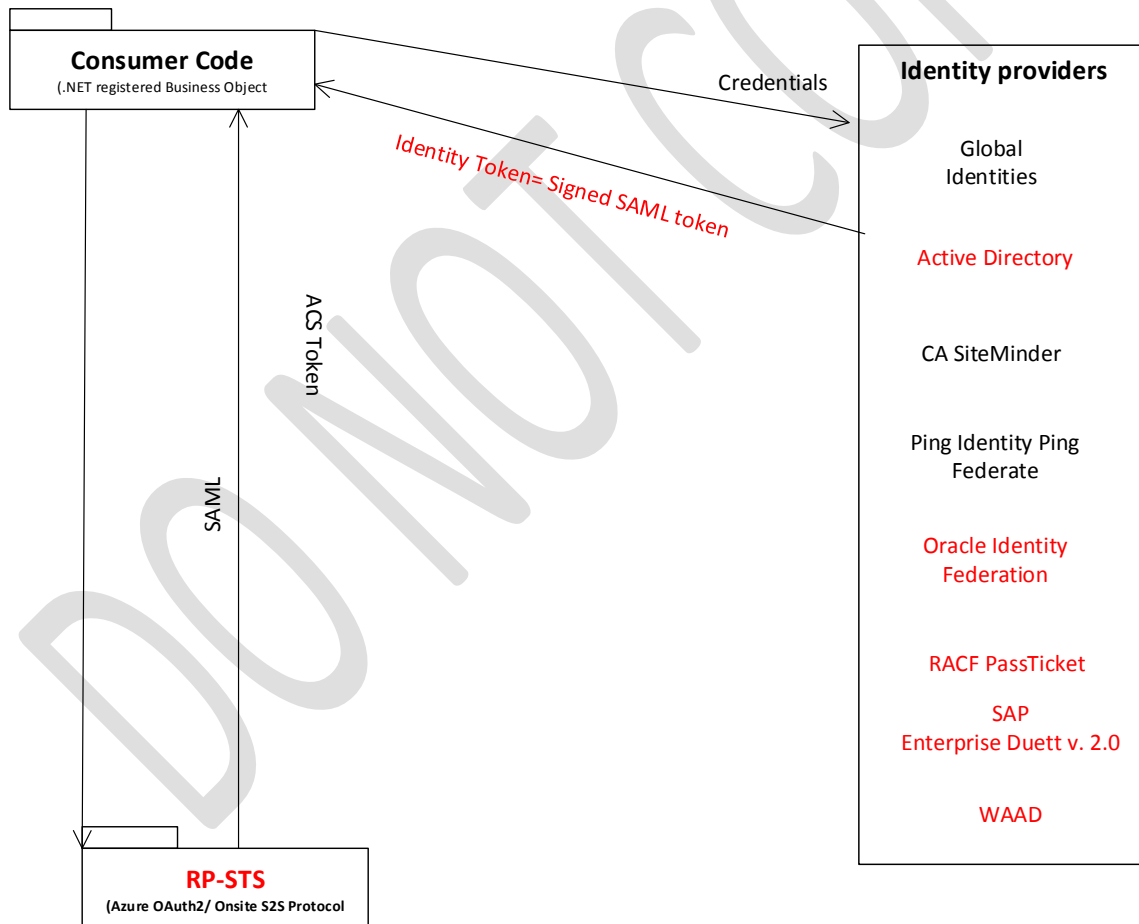
## 10. Standard Conversation - OOTB

### Enterprise wide Claims based Identity Management for Application (Standard Conversation – Fast/Reliable OOTB)



## 11. Enterprise wide Claims based Identity Management for Application & User

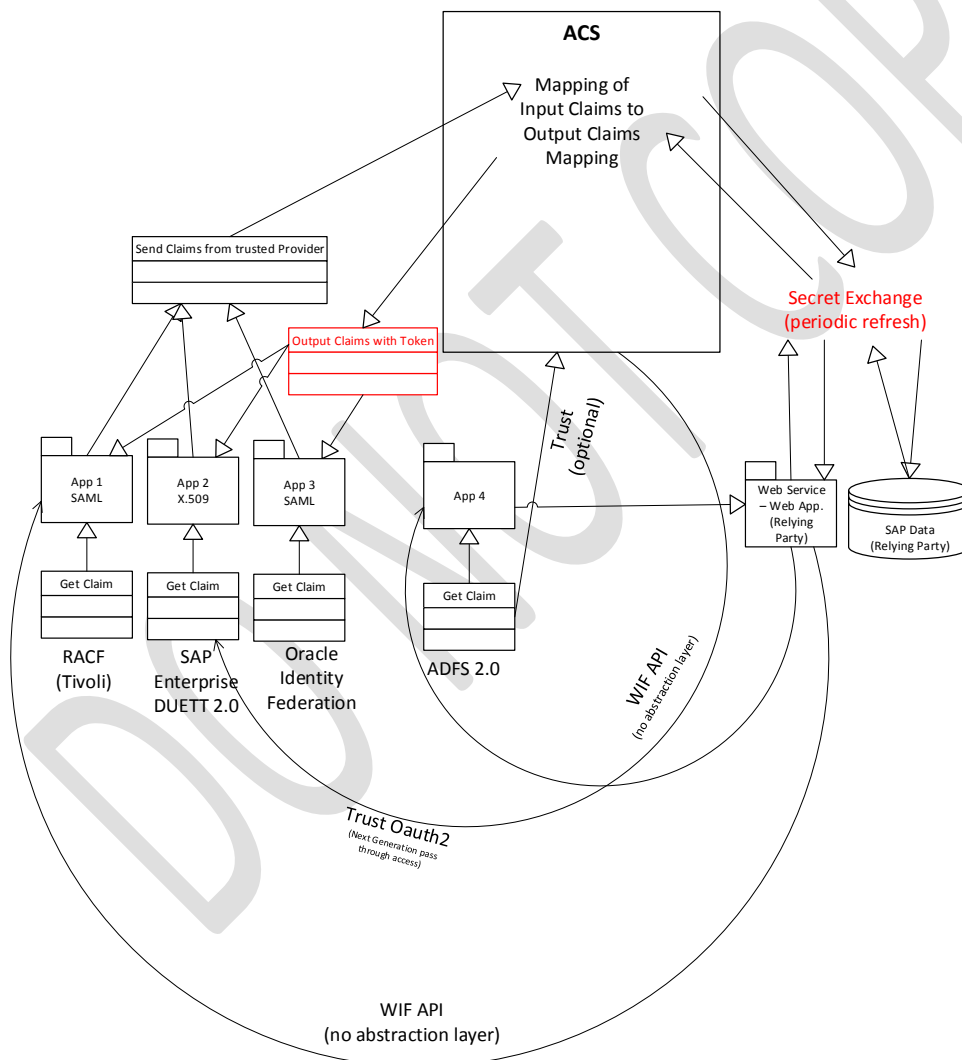
### Enterprise wide Claims based Identity Management for Application & User





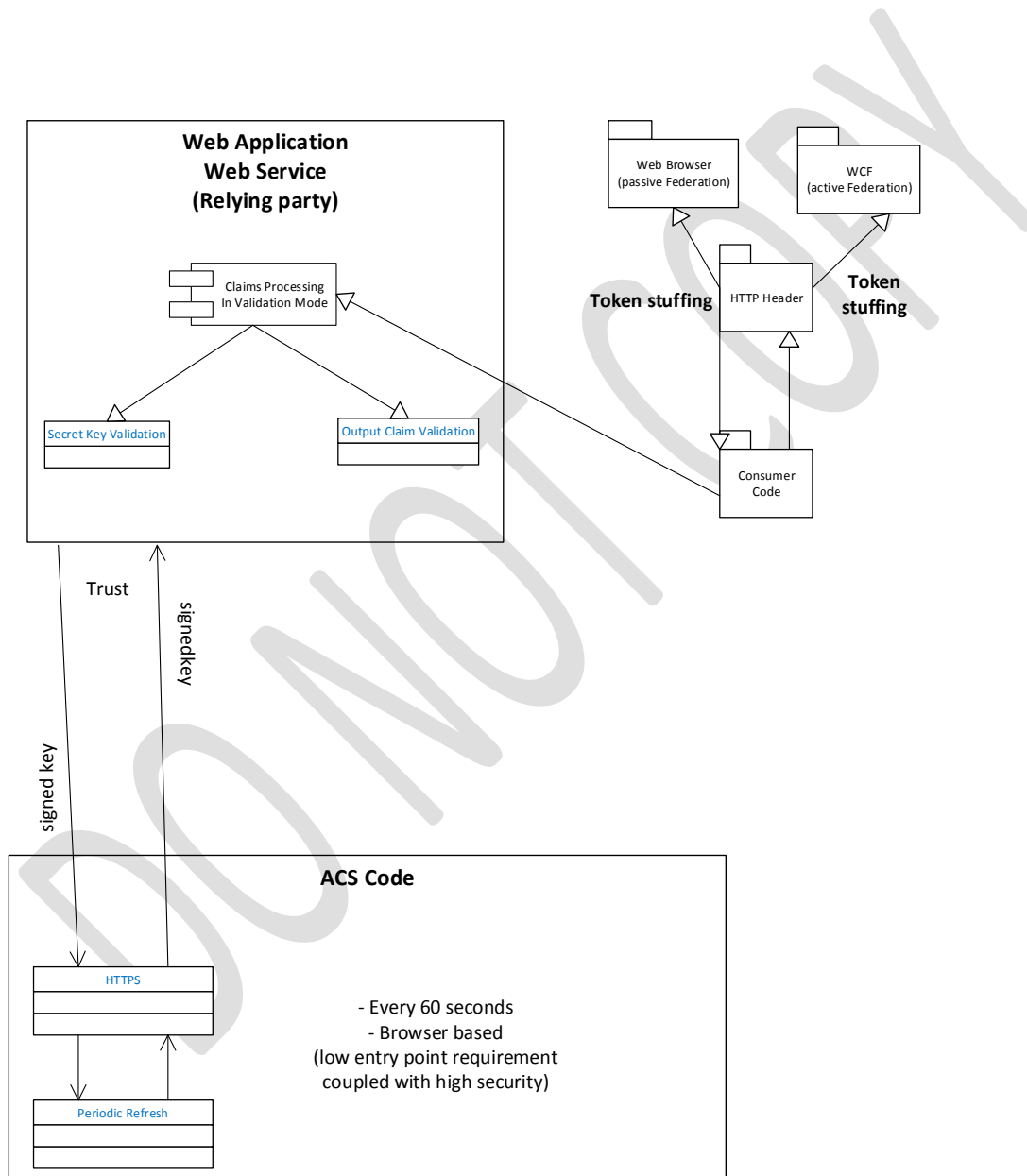
## 12. Claims based Identity Management for User welcome but just optional

### Enterprise wide Claims based Identity Management for Application (Claims based Identity Management for User welcome but just optional)



### 13. Minimum security procedure for external app interfacing

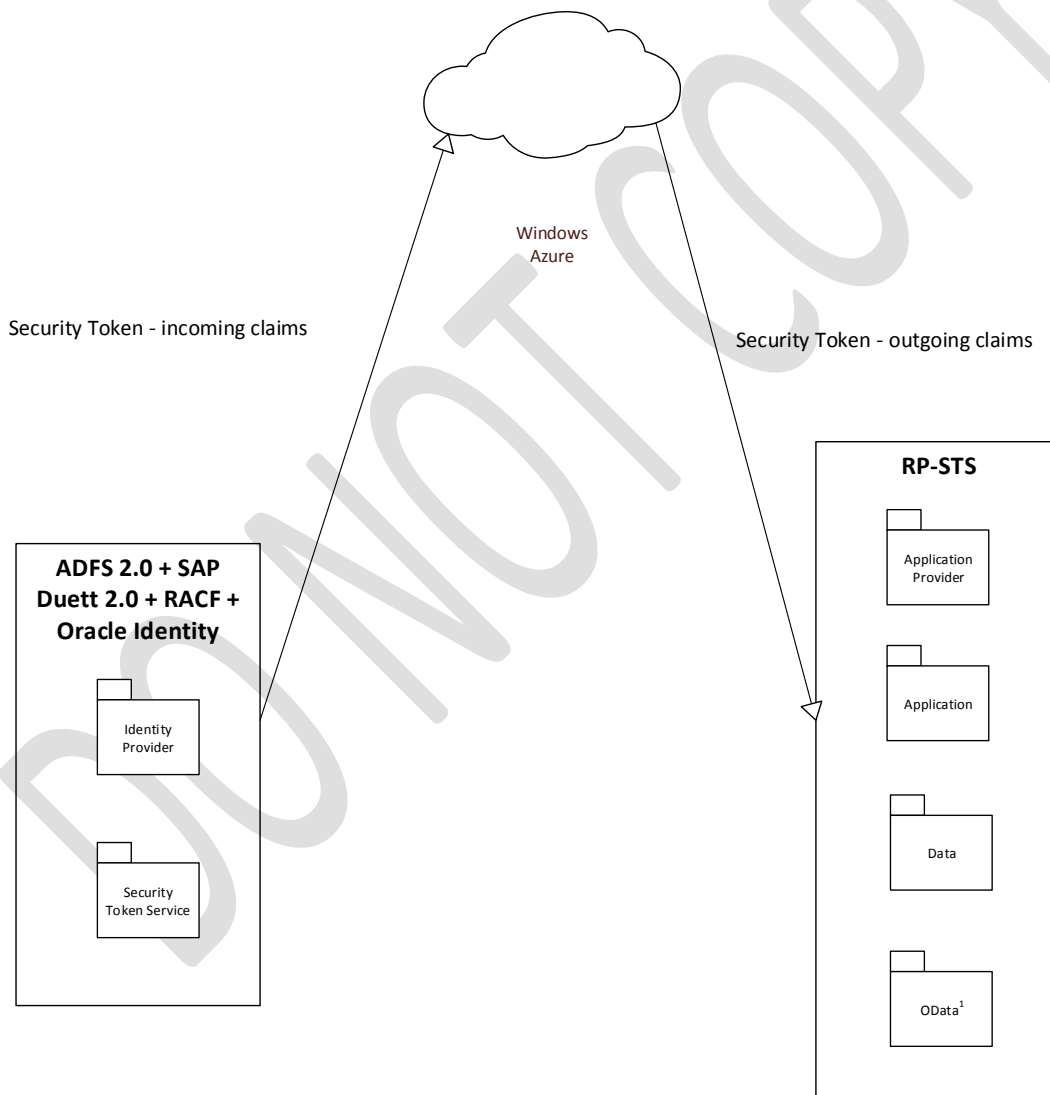
#### Enterprise wide Claims based Identity Management for Application (Minimum security procedure for external app interfacing)



## 14. Minimum security procedure for external app interfacing

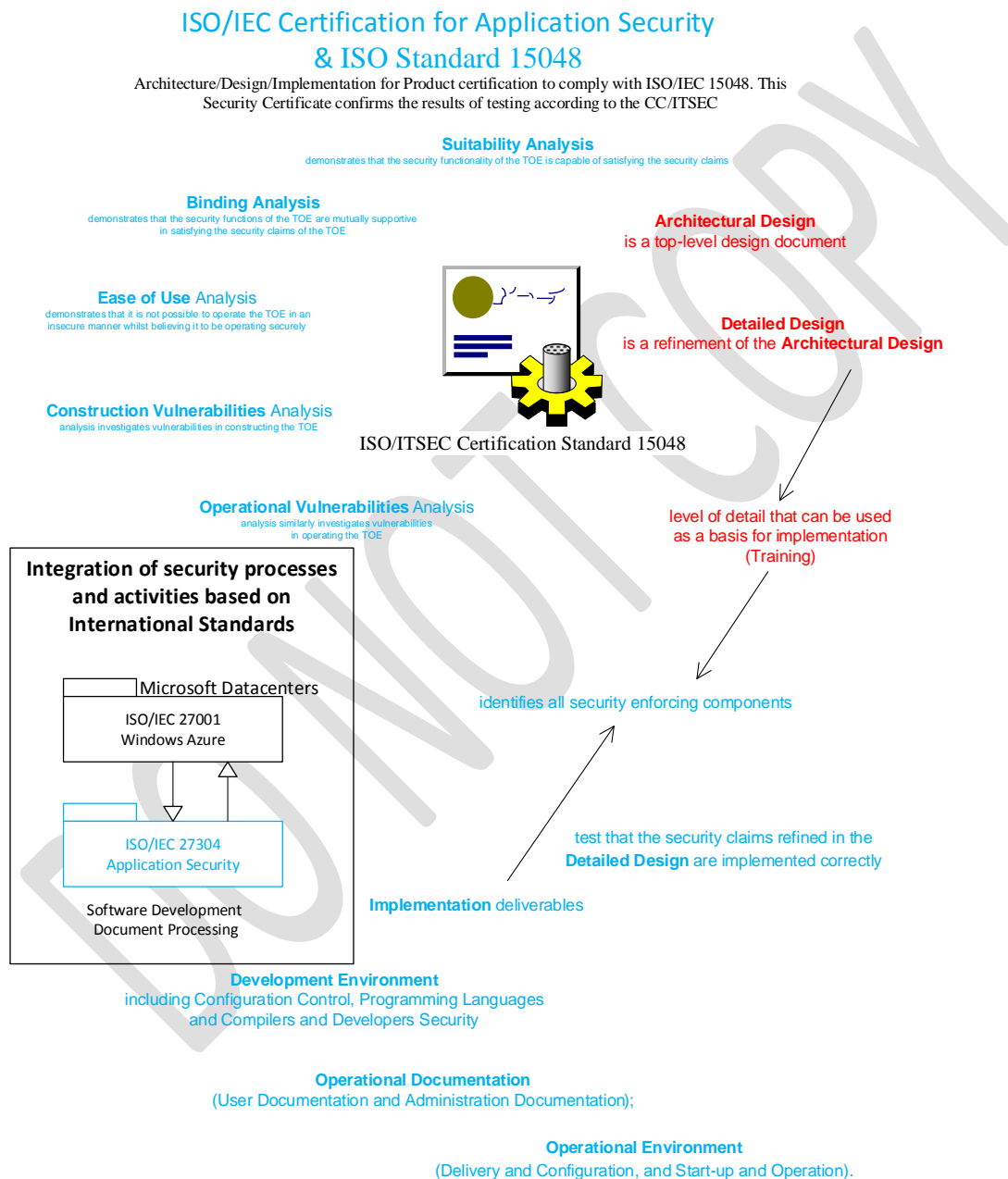
### AD+RACF+SAP<sup>1</sup>+Oracle Integration Delivering SAML/Oauth<sup>1</sup> Token for User

(Not capable to deliver SAML App Security)





## 16. Evidence that information being used or stored by applications is adequately protected



## 17. Corporate Binding Rule Scheme (CBRS)

# Corporate Binding Rule Scheme (CBRS)

