

SharePoint Saturday
Stockholm



Inside SharePoint Apps Security



Paolo Pialorsi - @PaoloPia

#SPSSTHLM17

February 14th, 2015

Platinum

NINTEX[®]

Gold

 **K2[®]**

Metalogix

cosign[®]

by *Arx*


Lunch

 **AvePoint[®]**

SharePint

knowit

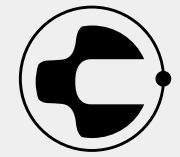
Silver



the power of smart process

 **RENCORE** **Cryptzone[™]** **KWizCom**
KNOWLEDGE WORKER COMPONENTS

alTran



CONSID

 **PERVASENT**

Web

 **SPDocKit**
by **acceleratio** **VisualSP[™]** **European
SharePoint
Conference** **Mail2Share** **pluralsight**
hardcore developer training

About me

- Project Manager, Consultant, Trainer
- About 50 Microsoft certification exams passed, including MC(S)M
- MVP Office 365
- Focused on SharePoint since 2002
- Author of 10 books about XML, SOAP, .NET, LINQ, and SharePoint
- Speaker at main IT conferences



@PaoloPia - paolo@pialorsi.com - <http://www.pialorsi.com/blog.aspx>

Agenda

- The big picture
 - Where do we come from?
 - Here we are!
- App Authentication
 - Internal
 - External
 - Server to Server / High Trust
- App Authorization
 - App Permissions
 - App-Only
 - On-the-fly Security

The big picture

Where do we come from?

- Full-trust solutions
 - Assemblies are in GAC (full-trust privileges)
 - Code runs with current user permissions
 - But can do `SPSecurity.RunWithElevatedPrivileges`
- Sandboxed solutions
 - Assemblies are in the Content DB
 - Execution restricted to the sandbox
 - Code Access Security determines permissions
 - Code always runs with current user permissions
 - No way to elevate security context!

Here we are!

- SharePoint 2013 authenticates security principals (as like as SP2010)
 - For which you can configure access control rules
- Security principals can be users or apps
 - User or Group/Role: SPPrincipal/SPUser/SPGroup
 - App: SPAppPrincipal (new in SP2013)

App authentication

App Authentication is supported
only for CSOM or REST API
requests originated by an app!

Authentication flavors for Apps

- Internal Authentication
- External Authentication via OAuth
- External Authentication via Server to Server

Internal Authentication

- When an app invokes CSOM/REST API from within an app web and with SAML token for user
- SharePoint-hosted apps use this kind of app authentication
- Cross-domain calls in Cloud-hosted apps use this kind of app authentication
- Does not support app-only authentication for elevation of privileges

DEMO

Internal App Authentication

Message Exception
 Non-Auth request. IsAuthenticated=True, UserIdentityName=0#.w\piasys\paolo.pialorsi, ClaimsCount=21

Uls RealTime(Correl...

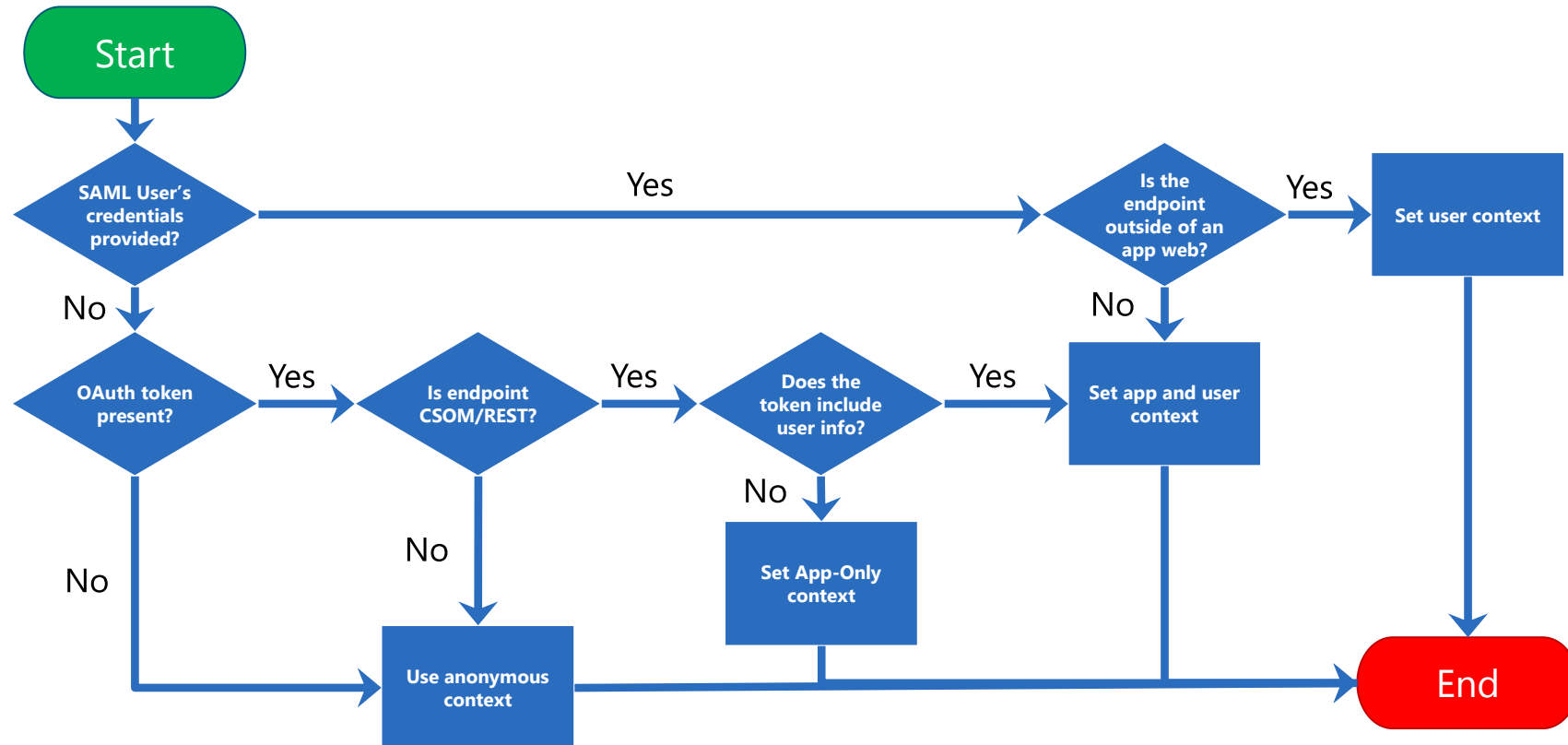
Time	Server	Process	Thread	Product	Category	EventID	Level	Correlation	Message	Name
05/23/2014 15:58:30.09		w3wp.exe (0x20E8)	0x2A8C	Share...	Microf...	aizmk	High	aebf939c-...	serviceHost_RequestExecuting	Request (POST:http://dev...
05/23/2014 15:58:30.09		w3wp.exe (0x20E8)	0x2A8C	Share...	Microf...	aizmj	High	aebf939c-...	serviceHost_RequestExecuted	Request (POST:http://dev...
05/23/2014 15:58:30.09		w3wp.exe (0x20E8)	0x2A8C	Share...	CSOM	agw11	Medium	aebf939c-...	End CSOM Request. Duration=19 milliseconds.	Request (POST:http://dev...
05/23/2014 15:58:30.09		w3wp.exe (0x20E8)	0x1E1C	Share...	Micro ...	uls4	Medium	aebf939c-...	Micro Trace Tags: 0 nasq,6 agb9s,5 agw10,0 aeg3c,11 ajnjd,6 ag69m,1 aizmk,0 aizmj,0 agw11	Request (POST:http://dev...
05/23/2014 15:58:30.09		w3wp.exe (0x20E8)	0x1E1C	Share...	Monito...	b4ly	Medium	aebf939c-...	Leaving Monitored Scope (Request (POST:http://devapps-3568613087e138.devapps.sharepoint-camp.com:80/sites/AppDevSit...	Request (POST:http://dev...
05/23/2014 15:58:30.10		w3wp.exe (0x20E8)	0x1D98	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.30		w3wp.exe (0x20E8)	0x2404	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.42		w3wp.exe (0x20E8)	0x23A8	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.42		w3wp.exe (0x20E8)	0x25C4	Share...	Monito...	nasq	Medium		Entering monitored scope (Request (POST:http://devapps-3568613087e138.devapps.sharepoint-camp.com:80/sites/AppDevSit...	
05/23/2014 15:58:30.42		w3wp.exe (0x20E8)	0x25C4	Share...	Loggin...	xmrv	Medium	aebf939c-...	Name=Request (POST:http://devapps-3568613087e138.devapps.sharepoint-camp.com:80/sites/AppDevSite/PiaSysSampleSP...	Request (POST:http://dev...
05/23/2014 15:58:30.42		w3wp.exe (0x20E8)	0x25C4	Share...	Authe...	agb9s	Medium	aebf939c-...	Non-Auth request. IsAuthenticated=True, UserIdentityName=0#.w\piasys\paolo.pialorsi, ClaimsCount=21	Request (POST:http://dev...
05/23/2014 15:58:30.42		w3wp.exe (0x20E8)	0x0380	Share...	CSOM	agw10	Medium	aebf939c-...	Begin CSOM Request ManagedThreadId=62, NativeThreadId=896	Request (POST:http://dev...
05/23/2014 15:58:30.43		w3wp.exe (0x20E8)	0x0380	Share...	Loggin...	xmrv	Medium	aebf939c-...	Site=/sites/AppDevSite	Request (POST:http://dev...
05/23/2014 15:58:30.43		w3wp.exe (0x20E8)	0x0380	Share...	App A...	ajnjd	Medium	aebf939c-...	Set the resolved app principal name to i:0.tims.sp.int 51d28445-2c28-49bc-b9dc-be2b2fcaafbd@7ac39c13-17e0-4d58-8365-ea2...	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x0380	Share...	Authe...	ag69m	Medium	aebf939c-...	TenantScopedPerm=0, AllowAppOnlyPolicy=False, AppId=i:0.tims.sp.int 51d28445-2c28-49bc-b9dc-be2b2fcaafbd@7ac39c13-1...	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x0380	Share...	Microf...	aizmk	High	aebf939c-...	serviceHost_RequestExecuting	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x0380	Share...	Microf...	aizmj	High	aebf939c-...	serviceHost_RequestExecuted	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x0380	Share...	CSOM	agw11	Medium	aebf939c-...	End CSOM Request. Duration=45 milliseconds.	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x1080	Share...	Micro ...	uls4	Medium	aebf939c-...	Micro Trace Tags: 0 nasq,3 agb9s,1 agw10,7 ajnjd,35 ag69m,1 aizmk,0 aizmj,0 agw11	Request (POST:http://dev...
05/23/2014 15:58:30.47		w3wp.exe (0x20E8)	0x1080	Share...	Monito...	b4ly	Medium	aebf939c-...	Leaving Monitored Scope (Request (POST:http://devapps-3568613087e138.devapps.sharepoint-camp.com:80/sites/AppDevSit...	Request (POST:http://dev...
05/23/2014 15:58:30.57		w3wp.exe (0x20E8)	0x1D50	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.66		w3wp.exe (0x20E8)	0x1ABC	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.77		w3wp.exe (0x20E8)	0x1A34	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.79		w3wp.exe (0x20E8)	0x2620	Share...	Micro ...	uls4	Medium		Micro Trace Tags: (none)	
05/23/2014 15:58:30.88		NodeRunnerAnalytics...	0x177C	Search	Searc...	aiy1k	Medium		Microsoft.Ceres.CoreServices.Node.NodeController : No constellate operation queued for 2 minutes, returning from Dequeue	
05/23/2014 15:58:30.88		NodeRunnerAnalytics...	0x177C	Search	Searc...	aiy1p	Medium		Microsoft.Ceres.CoreServices.Node.NodeController : Dequeued returned	
05/23/2014 15:58:30.88		NodeRunnerAnalytics...	0x177C	Search	Searc...	aiy1o	High		Microsoft.Ceres.CoreServices.Node.NodeController : Already configured with version (poll) 4	
05/23/2014 15:58:30.88		NodeRunnerAnalytics...	0x177C	Search	Searc...	aiy1r	Medium		Microsoft.Ceres.CoreServices.Node.NodeController : Completed (Re)Constellate	
05/23/2014 15:58:30.88		NodeRunnerAnalytics...	0x177C	Search	Searc...	aiy1j	Medium		Microsoft.Ceres.CoreServices.Node.NodeController : Dequeue invoked	
05/23/2014 15:58:31.86		OWSTIMER.EXE (0x...	0x0794	Share...	Monito...	nasq	Medium	2922e7f2-...	Entering monitored scope (Timer Job job-upgrade-sites). Parent No	
05/23/2014 15:58:31.86		OWSTIMER.EXE (0x...	0x0794	Share...	Loggin...	xmrv	Medium	afbf939c-...	Name=Timer Job job-upgrade-sites	Timer Job job-upgrade-sites

[AutoScroll here..]

External Authentication via OAuth

- The app invokes CSOM/REST API providing an access token signed by Azure ACS
 - Bearer token in Authorization HTTP header
- The access token can include app and user identity
- The access token can be an app-only identity
- Is the only “External Authentication” model supported by Microsoft Office 365

SharePoint 2013 Apps' Authentication



The OAuth Protocol

- The OAuth 2.0 authorization framework enables a third-party application to obtain **AuthZ Rules** to an **CSOM/REST**, either **on behalf of a user** by orchestrating an approval interaction between the resource owner and the HTTP service, **or by allowing the third-party application to obtain access to act as app-only.**
- <http://tools.ietf.org/html/rfc6749>

Security Tokens used in OAuth

- Context Token
 - Contextual information passed to the app
- Refresh Token
 - Used by client app to acquire an access token
- Access Token
 - Token passed to SharePoint from the app when using external authentication
- Authorization Code
 - Used to register an app with on the fly permissions (more later ...)

SPAAppToken: inside OAuth context token

```
{ "typ": "JWT", "alg": "HS256" } { "aud": "a683fa34-b747-48cd-adc8-bfca2778684b/...@786dcab-5543-431d-a979-f5b7cd4912df", "iss": "00000001-0000-0000-c000-000000000000@786dcab-5543-431d-a979-f5b7cd4912df", "nbf": "1400800147", "exp": "1400843347", "appctxsender": "00000003-0000-0ff1-ce00-000000000000@786dcab-5543-431d-a979-f5b7cd4912df", "appctx": "{ \"CacheKey\": \"tRQ5KjLuuZ0X5b6rE37QaGHKJCoPZ4XGi3LuvA1CGhs=\", \"SecurityTokenServiceUri\": \"https://accounts.accesscontrol.windows.net/tokens/OAuth/2\" }", "refreshtoken": "IAAAP7zm7YVpxhrwPyWr6wuVt1zoJDpXTmUGyBeyXQZtclolc459ra5meHNaCiKlfEsmhiLGk8hTjmVLBNZRT-pOqsf7VxdM2WKtY3Gt06cHqGgcbvYDXDYG2VuOGMiUrQTEdOYMM1Uvg6bDdBillamOI7KeG3SLzBxOfxCy1UQLFlq_4z1iSggz-SFbUuNELJdj3atd3gwCOHbLTfBETp9oOT55R6WF2-GiY6WLoHG2OsyDDulzm2dniCvxqguUKOtvZsD33-w2Mj-vJpkLrueAesHXmHANKOcw2mAQ-APx9UppCYOdyYIsZtZReimx0uTJ5JpnejfIolnGyBp5Z_UY", "isbrowserhostedapp": "true" }
```

Azure AD (Microsoft Entra ID) URI

Key	Value
aud	a683fa34-b747-48cd-adc8-bfca2778684b/...@786dcab-5543-431d-a979-f5b7cd4912df
iss	00000001-0000-0000-c000-000000000000@786dcab-5543-431d-a979-f5b7cd4912df
nbf	22/05/2014 23:09:07
exp	23/05/2014 11:09:07
appctxsender	00000003-0000-0ff1-ce00-000000000000@786dcab-5543-431d-a979-f5b7cd4912df
appctx	{ \"CacheKey\": \"tRQ5KjLuuZ0X5b6rE37QaGHKJCoPZ4XGi3LuvA1CGhs=\", \"SecurityTokenServiceUri\": \"https://accounts.accesscontrol.windows.net/tokens/OAuth/2\" }
refreshtoken	IAAAP7zm7YVpxhrwPyWr6wuVt1zoJDpXTmUGyBeyXQZtclolc459ra5meHNaCiKlfEsmhiLGk8hTjmVLBNZRT-pOqsf7VxdM2WKtY3Gt06cHqGgcbvYDXDYG2VuOGMiUrQTEdOY...
isbrowserhostedapp	true

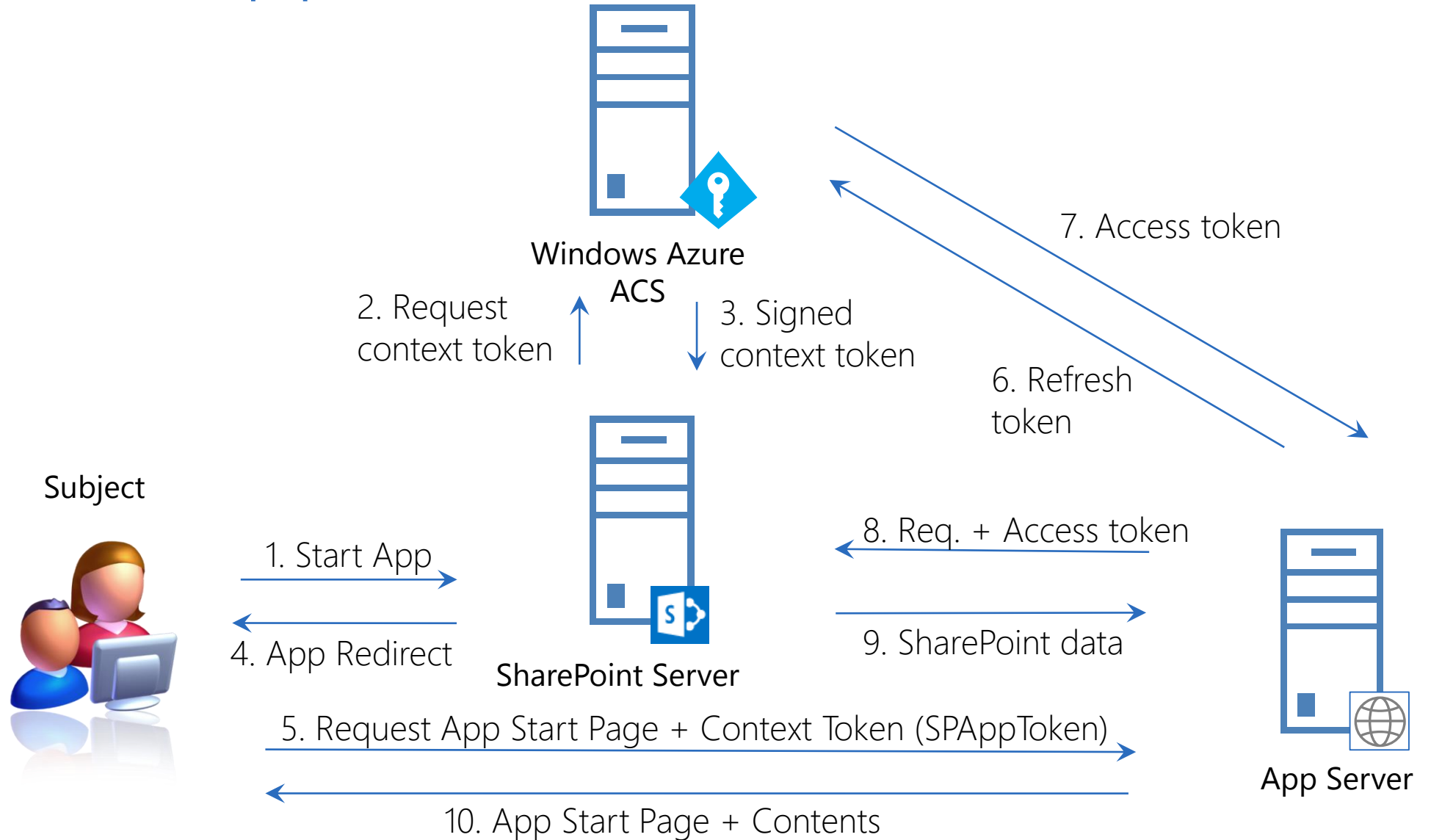
Credits: <http://blogs.msdn.com/b/kaevans/archive/2013/04/05/inside-sharepoint-2013-oauth-context-tokens.aspx>

DEMO

External App Authentication via OAuth
on Microsoft Office 365 + Fiddler

SharePoint Apps

OAuth Flow



External app Authentication via S2S

- The app invokes CSOM/REST API providing an access token signed with a trusted X.509 certificate
 - App code requires access to private key of certificate
- Leverages a direct trust between SharePoint and an app (further details later ...)
- Is only supported on-premises

Server to Server (High Trust)

- High Trust != Full Trust
 - Extension to OAuth
 - Leveraged by apps and infrastructural services (Workflow Manager, Exchange, etc.)
 - Can use any user identity, self issued and signed access token
- Direct trust relationship
 - Between SharePoint and the external app/service
 - Based on X.509 certificates
 - One certificate for each app (avoid sharing certs across apps)
 - Can leverage shared certificates for Trust Brokers (development environments)
- Available for Provider-hosted apps
 - Supported by wizard of Visual Studio 201x and Office Developer Tools for VS
 - Configurable by using PowerShell

Registration Steps

- Create an X.509 certificate (self-signed is ok)
- Register public key in SharePoint and create a trusted security token issuer based on that public key (via PowerShell)
 - Manually (via .cer file)
 - Automatically (via endpoint metadata URL)
- Create a provider-hosted app with access to the private key
- Use the TokenHelper class to create S2S access tokens
- Pass the access token to CSOM/REST API

DEMO

External App Authentication via S2S on-premises

App Principals

- Are tenancy-scoped account for app identity
 - In a single-tenant farm, which is the default for on-premises, are farm-scoped
- Represented as a registered GUID
 - Using AppRegNew.aspx page
 - Using PowerShell
 - Using the Seller Dashboard

Managing App Principals

- AppRegNew.aspx
 - Allows manual registration of a new app principal
 - Client ID: GUID identifier for app principal
 - Client Secret: (not used in S2S)
 - App Host Domain: Base URL of remote web
 - Redirect URL: used to configure on-the-fly security (more on this shortly ...)
- AppPrincipals.aspx
 - Enumerates all the registered apps, together with their unique client IDs
- AppInv.aspx
 - Allows retrieving app registration information from an app ID
 - Allows setting custom permissions to already registered app principals

DEMO

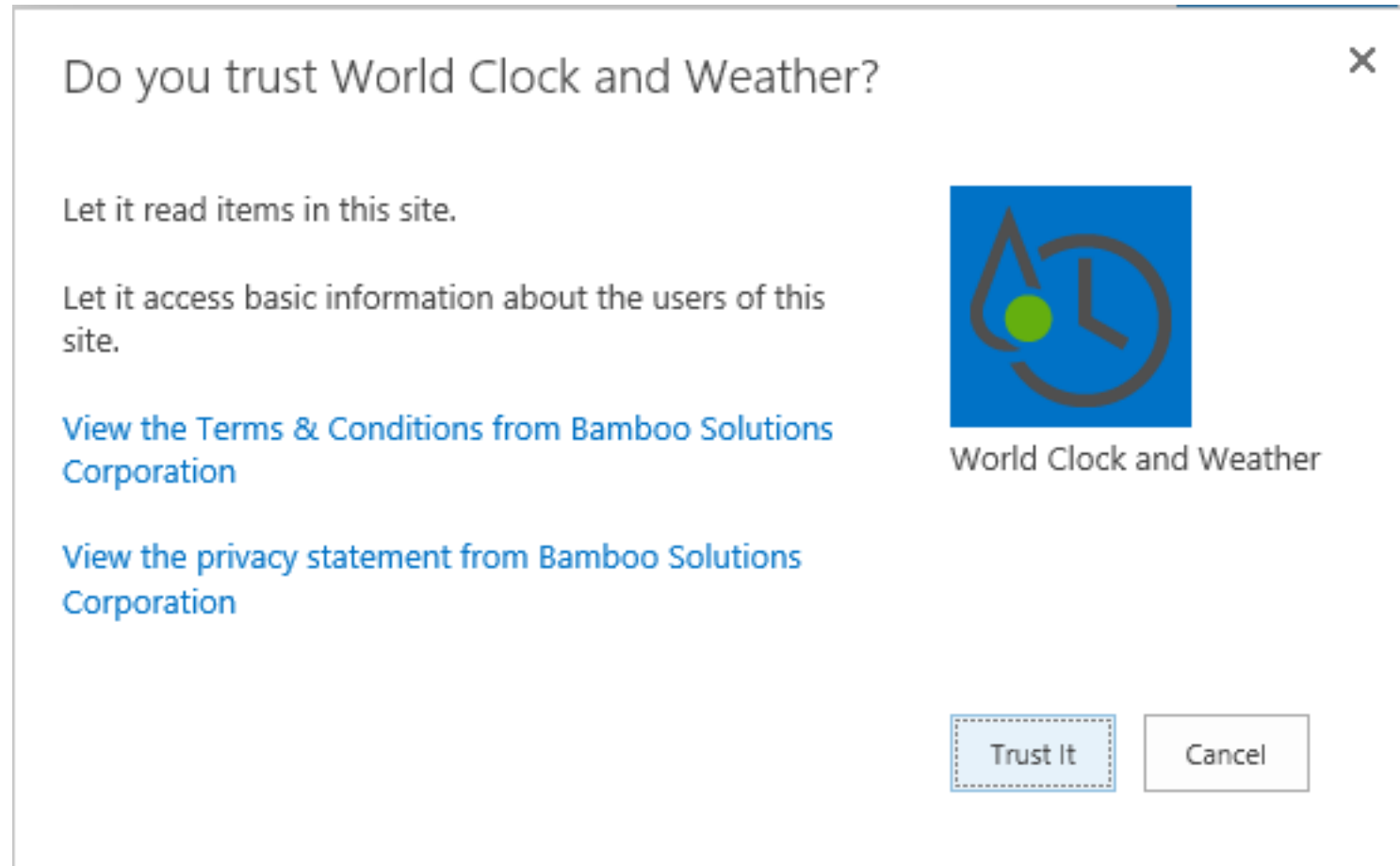
App*.aspx pages

App Authorization

App Permissions

- Are different from user permissions
- Are granted as all or nothing
 - App can include permissions requests in application manifest
 - Installing user grants/denies permissions during installation
 - If permissions request denied, SharePoint does not install the app
- Users can grant only permissions that they have
 - You must be at least a Site Owner to install an App
- Cannot be changed after assignment
 - Permissions can only be revoked

Trusting an App



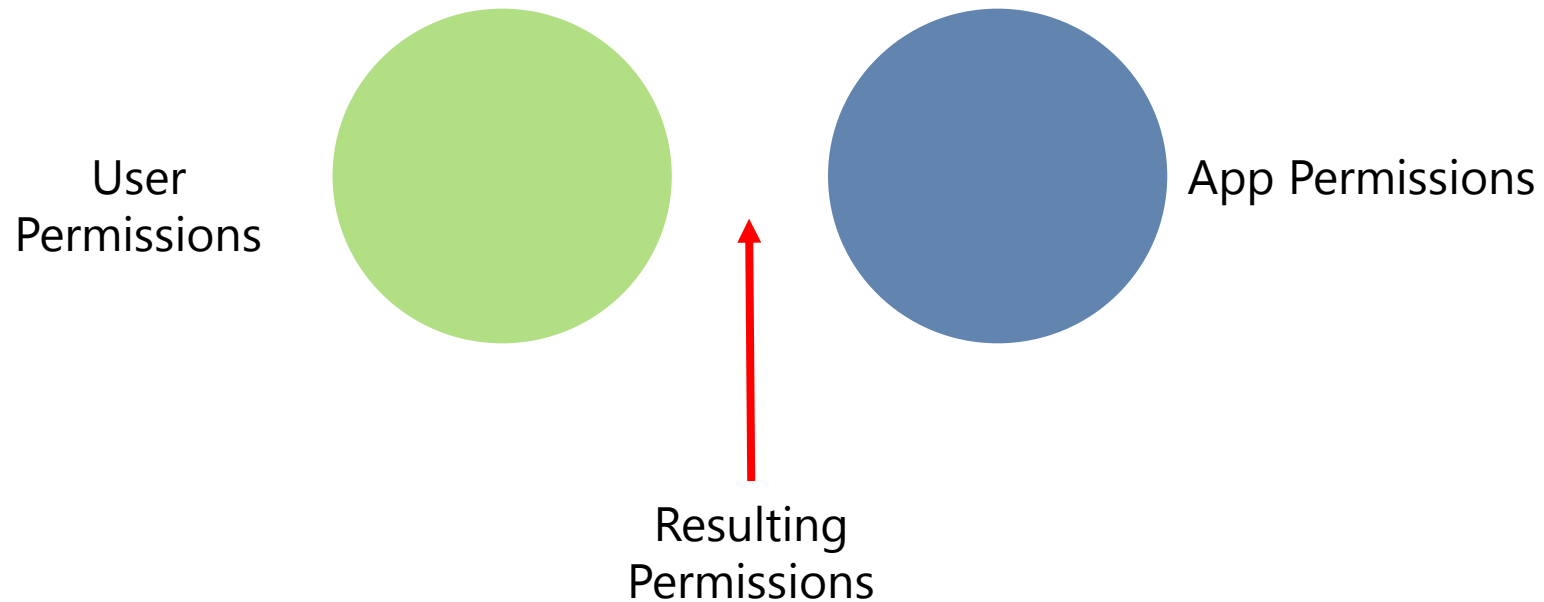
More about App Permissions

- App has full control over its app web
 - But no other default permissions
 - No default access to host web, for instance ...
- Every Permission is made of Scope and Right
 - Permission Scopes
 - Site Collection, Web Site, List, Tenant, Services (Search, Managed Metadata, User Profile, etc.)
 - Permissions applied to a target scope, apply also to all the children of that scope
 - Permission Rights
 - Read-Only, Write, Manage, Full Control
 - Other specific rights for Services
 - Apps Rights and Scopes are not customizable

Scope URI	Scope Alias	Available Rights
http://sharepoint/content/sitecollection	Site	Read, Write, Manage
http://sharepoint/content/sitecollection/web	Web	Read, Write, Manage
http://sharepoint/content/sitecollection/web/list	List	Read, Write, Manage
http://sharepoint/content/tenant	AllSites	Read, Write, Manage
http://sharepoint/bcs/connection	None (currently not supported)	Read
http://sharepoint/search	Search	QueryAsUserIgnoreAppPrincipal
http://sharepoint/projectserver	ProjectAdmin	Manage
http://sharepoint/projectserver/projects	Projects	Read, Write
http://sharepoint/projectserver/projects/project	Project	Read, Write
http://sharepoint/projectserver/enterprisesresources	ProjectResources	Read, Write
http://sharepoint/projectserver/statusing	ProjectStatusing	SubmitStatus
http://sharepoint/projectserver/reporting	ProjectReporting	Read
http://sharepoint/projectserver/workflow	ProjectWorkflow	Elevate
http://sharepoint/social/tenant	AllProfiles	Read, Write, Manage
http://sharepoint/social/core	Social	Read, Write, Manage
http://sharepoint/social/microfeed	Microfeed	Read, Write, Manage
http://sharepoint/taxonomy	TermStore	Read, Write

Default permission model

- By default an app uses a token corresponding to:
 - App permissions
 - User permissions



App-Only Permissions

- An App can call CSOM/REST API as “app-only”
 - To make elevation of privileges
 - The app-only can have permissions greater than the current user
 - To call SharePoint when there isn't a current user
 - Callback, remote event receivers, batches, timer jobs, etc.
- Has to be declared in the app manifest
 - AllowAppOnlyPolicy attribute in AppPermissionRequests
 - Need some code to acquire an app-only access token
 - You can leverage the TokenHelper class to achieve this result

On-the-fly Security

- Suitable for pre-registered apps
 - Seller Dashboard or AppRegNew.aspx
 - The redirect URI is mandatory in this case
 - Has to be over HTTPS
- ACS is required, thus it targets Office 365 *mainly*
- App invokes OAuthAuthorize.aspx and gets back an Authorization Code
 - Via querystring for redirect URI
- Using the Authorization Code can get an on-the-fly Access Token
- This type of app can only be run by users who have Manage permissions to the resources the app wants to access
- An app that request permission to access SharePoint resources on-the-fly can't request Full Control right.

DEMO

On-the-fly Security

Please rate this session...

...and visit our sponsors who made this day possible!



Thank you!

RATE THIS SESSION



AWESOME



OK



MEH

This session: www.spsstockholm.com/17

Overview: www.spsstockholm.com/rate

