



SAP MOBILE: ATTACK & DEFENSE

Julian Rapisardi
jrapisardi@onapsis.com

Fernando Russ
fruss@onapsis.com



This presentation contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

Company mission is to **secure business-critical applications**.

Transforming how organizations protect the applications that manage their **business-critical processes and information**.

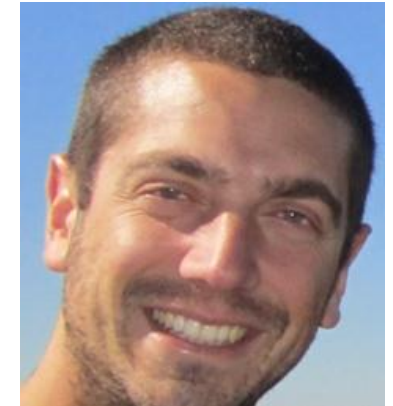
- *Founded:* 2009
- *Locations:* Buenos Aires, AR | Boston, MA | Munich, DE | Lyon, FR
- *Research:* 200+ SAP security advisories and presentations published
- *What does Onapsis do?*
 - Innovative business-critical applications security software
 - Trainings and presentations on business-critical infrastructure security

Who are we?



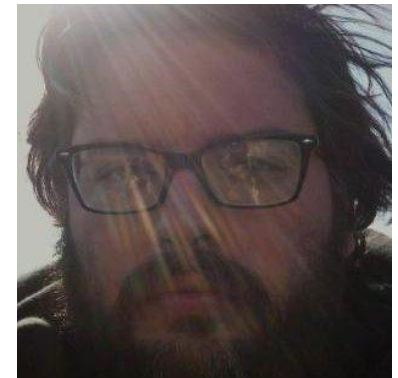
- Julian Rapisardi **SAP Security Specialist @ Onapsis**

- Background on SAP Security Assessments
- Has been involved in several SAP GRC projects



- Fernando Russ **Senior Researcher @ Onapsis**

- Background on Penetration Testing and Vulnerabilities Research
- Reported vulnerabilities in different SAP and Oracle Products



- Both Authors/Contributors on diverse posts and publications
- Speakers and Trainers at Information Security Conferences

- Introduction
 - Context
 - History
- SAP Mobile
 - SMP (SAP Mobile Platform)
 - SAP Fiori
- Attack surface
- Architecture Overview
- Security challenges while building our application
- Conclusions



Introduction

So...what is SAP?

SAP (*Systems, Applications and Products in Data Processing*) is a German company devoted to the development of business solutions.

- Founded in 1972
- 75.000 employees
- More than 291.000 customers in 190 countries
- *Working with Global Fortune-500 companies and large governmental organizations*

SAP systems store and process the most critical business information.

If the SAP platform is breached, an intruder would be able to perform:

ESPIONAGE

Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.

SABOTAGE

Paralyze the operation of the organization by shutting down the SAP system, disrupting interfaces with other systems and deleting critical information, etc.

FRAUD







Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

As part of the industry's push towards remotely accessible business functions, SAP has been evolving their business critical applications to this trend.

Going mobile brings some security challenges, such as:

- Choosing adequate authentication mechanisms
- Securing communications
- Defining proper data encryption requirements

SAP Mobile Platforms have travelled several miles in SAP history.

2010	2011	2012	2013
		 	 
<p><i>SAP buys Sybase</i></p> <p>Sybase is SAP's largest acquisition ever.</p>	<p><i>Sybase Unwired Platform (SUP)</i></p> <p>Supports integration with SAP NetWeaver Gateway via OData.</p>	<p><i>SAP buys Syclo</i></p> <p>Syclo's Agency, another mobile product (supporting Online and Offline Capabilities).</p> <p><i>Mobile Analytics Kit</i></p>	<p><i>SAP Mobile Platform 3.0 (SMP3) unifies SUP, Syclo Agency and SAP's mobile technologies into one mobile platform.</i></p>

SAP Mobile

SAP Financial Fact Sheet NY/NJ SBHC Volunteers SAP Mobile Platform SAP System Monitoring SAP Retail Execution Hybrid Web Container SAP Fiori Client SAP Support Desk SAP CRM Sales SAP Transport Notification and Status SAP Sales Manager SAP Travel Expense Report SAP Sales OnDemand SAP EMR Unwired SAP Cart Approval SAP Inventory Manager SAP Direct Store Delivery SAP Learning Assistant SAP Mobile Utilities SAP Learn Now SAP Sales Companion SAP IT Incident Management SAP Retail Execution Mobile SAP Rounds Manager SAP Business Objects SAP Job Progress Monitor SAP Business Objects Mobile SAP Visual Enterprise Viewer SAP Cloud for Travel & Expense SAP RealSpend SAP TM Notifier Sybase Mobile Workflow 1 SAP Sales Pipeline Simulator SAP Customer Financial Fact Sheet SAP Authenticator SAP Work Manager for Maximo SAP CRM SERVICE MANAGER SAP Cloud for Customer SAP GRC Access Approver SAP Manager Insight SAP Commissions Check SAP Mobile Documents SAP Collections Insight SAP HR Approvals SAP Utilities Customer Engage SAP Customer Loyalty SAP IT Change Approval SAP Business ByDesign SAP BusinessObjects Mobile Visual Enterprise MOB SAP FIORI SAP Work Manager SAP Travel Receipt Capture SAP User Experience Monitor SAP Patient Management SAP CRM SALES Sybase Data Provider 2.1.1 SAP Solution Manager Mobile Apps SAP Receivables Manager SAP End User Experience Monitoring SAP Enterprise Support Academy SAP CRM Service Manager SAP Customer Briefing SAP Shopper Experience

64 apps
(Just for Android)

SAP's mobile enterprise solutions are various.

Most used ones today are *SAP Fiori* and *SAP Mobile Platform (SMP)*.

SAP Fiori is a collection of pre-built mobile applications, delivered via the SAP Store.

SMP is used to build and deploy mobile applications across a range of mobile devices. It is a middleware platform, which enables users to connect the existing enterprise systems or applications with the mobile devices.

Let's get a deeper look at them..

SAP Fiori | Lines of business



Finance

- Accounts Payable Accountant
- Accounts Payable manager
- Accounts Receivable Accountant
- Accounts Receivable Manager
- Cash Manager
- Controller
- G/L Accountant
- Manager
- Access Control Administrator
- Financial Close Manager
- Employee
- Senior Executive

Human Resources

- Employee
- Manager

Asset Management

- Maintenance Worker & Planner
- EHS-Production Worker
- EHS-Foreman

Sales

- Sales (CR)
- Sales
- Internal Rep
- Manager
- Manager
- Manager
- Contract Rec

The screenshot shows the SAP Fiori 'My Home' dashboard for a user named Peter Gasston. The dashboard is organized into several key areas:

- My Home Header:** Displays the user's name (Peter Gasston), employee ID (3), and a 'Leave Requests' indicator showing 1 request.
- Comparative Annual Totals:** A bar chart showing revenue by region: Americas (234 M), EMEA (97 M), and Germany (197 M).
- Approve Travel Request:** A card with a large '1' and an airplane icon, indicating one pending request.
- Gross Revenue:** A card showing 'Global - Year to Date' revenue of 348.2 M USD (Actual).
- Cumulative Totals Expenses:** A card showing a bar chart for 'Actual and Target' expenses, with a value of 125 M EUR.
- MRP Cockpit:** A central section with five monitoring cards:
 - Uncovered Sales Orders Monitor: 98 Percent.
 - Materials with Shortages Monitor: 368 Materials.
 - Late Purchase Orders Monitor: 103 Items.
 - Late POs from Asia: 103 Items.
 - Uncovered Sales Orders Next 5 Days: 6,576 US Dollars.

SAP Fiori is a collection of apps for frequently used SAP functions (Finance, HR, Sales & Marketing, Procurement, Manufacturing, Supply Chain etc.) that work across devices – desktop, tablet, or smartphone.

SAP Fiori landscape includes:

- SAP backend systems
- SAP NetWeaver Gateway
- SAP UI5 (UI development toolkit for HTML5) for NetWeaver

No mobile platform is required

Sybase Unwired Platform and the *Syclo Agency* development platform have been integrated, and the product rebranded to *SAP Mobile Platform (SMP)*.

SMP landscape includes:

SAP backend systems

- SAP ERP (Enterprise Resource Planning)
- SAP CRM (Customer Relationship Management)
- SAP SCM (Supply Chain Management)
- SAP SRM (Supplier Relationship Management)

NetWeaver Gateway for providing interfaces to business logic

SMP to store and pass data between NetWeaver Gateway and mobile devices

Afaria assists managing and securing mobile devices, across platforms.

Attack surface

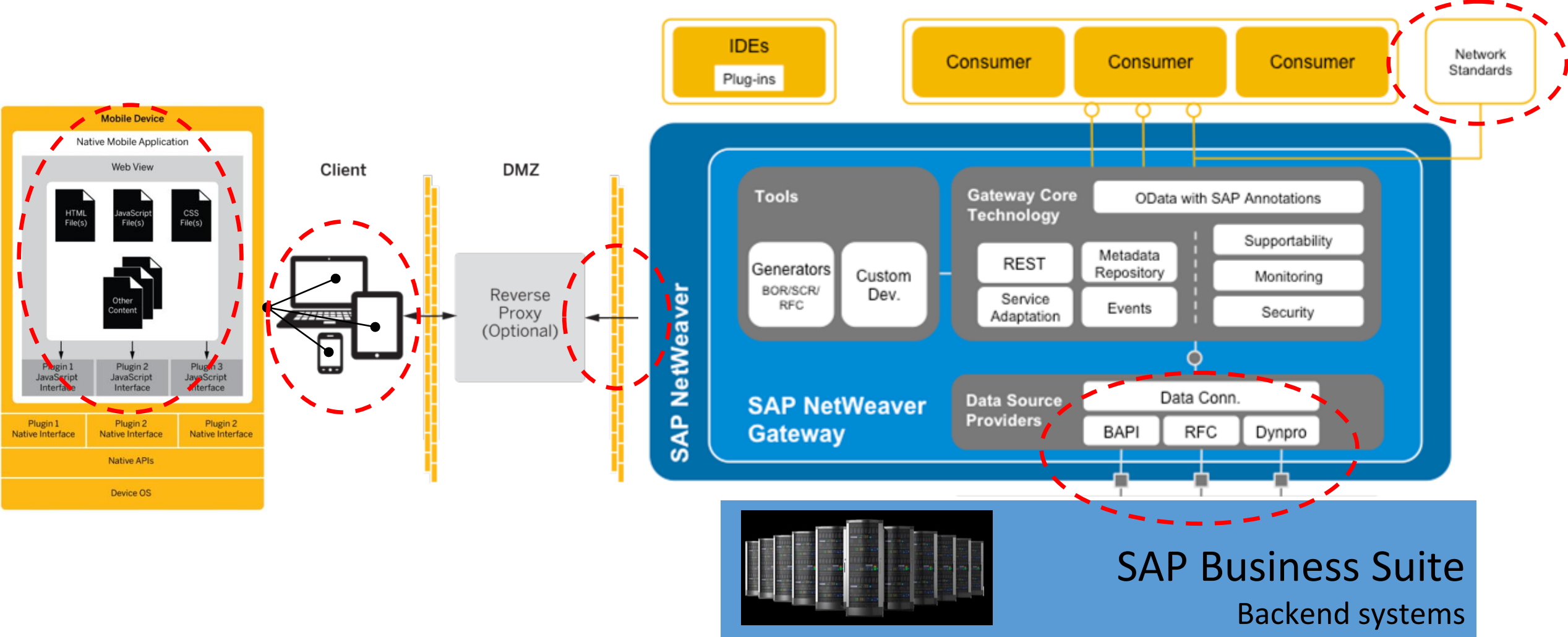
The App lets you browse the bookings of a series of airline carriers, based on the flight connection available in certain periods of time. (as enhancement is planned to show the receipt as a Fiori plug in).

- **Rotten by design™ :)**
- Implemented using...
 - Apache Cordova 4.3.0 + Kapsel (using SMP 3.0 SP08)
 - SAP Fiori Wave 1 SP02
 - SAP Netweaver Gateway (SAP EHP 2 for SAP NetWeaver 7.0)
 - SAP IDES (EHP6 FOR SAP ERP 6.0)

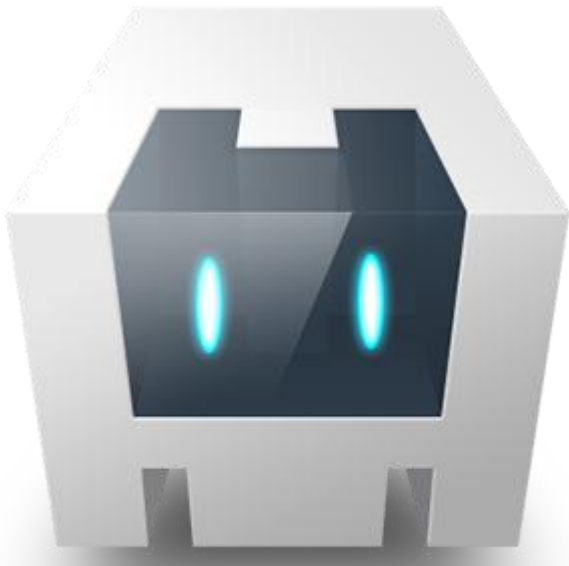


Architecture Overview

Our Architecture



Apache Cordova is a platform for building native mobile applications using HTML, CSS and JavaScript.



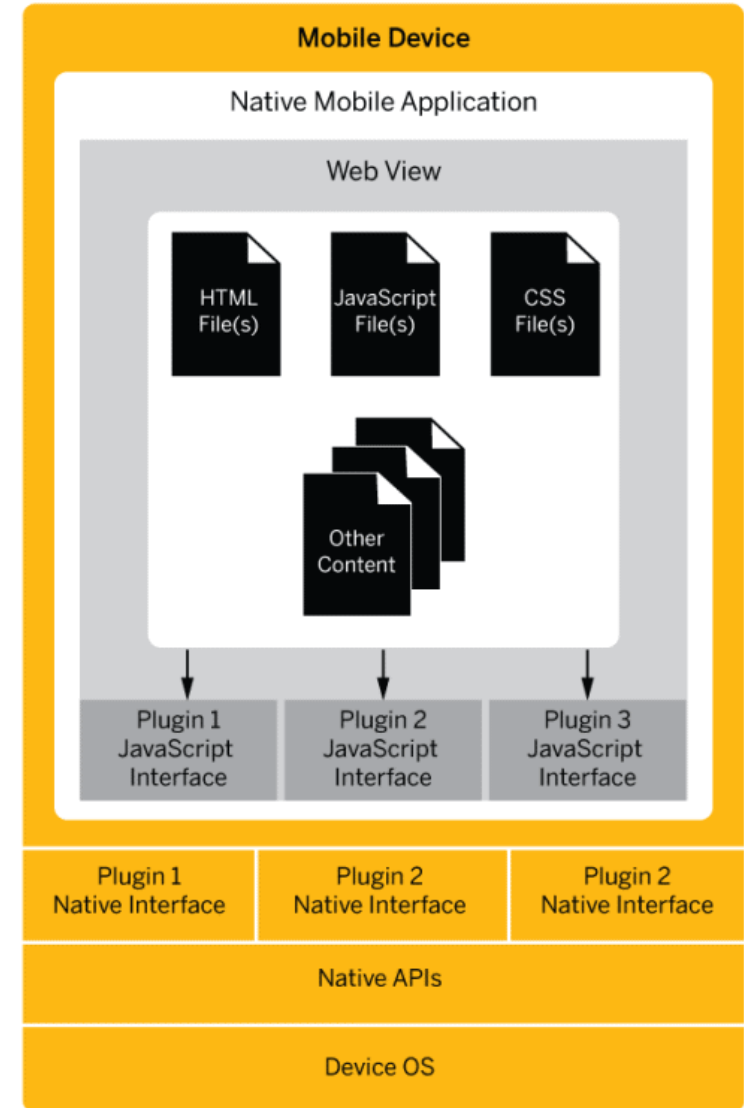
- Open source technology
- Supports ~ 15 Platforms
 - Android
 - IOS
 - Windows Phone
 - ...

<https://cordova.apache.org/>

A serie of Apache Cordova plugins that enhance it allowing interactions with SAP

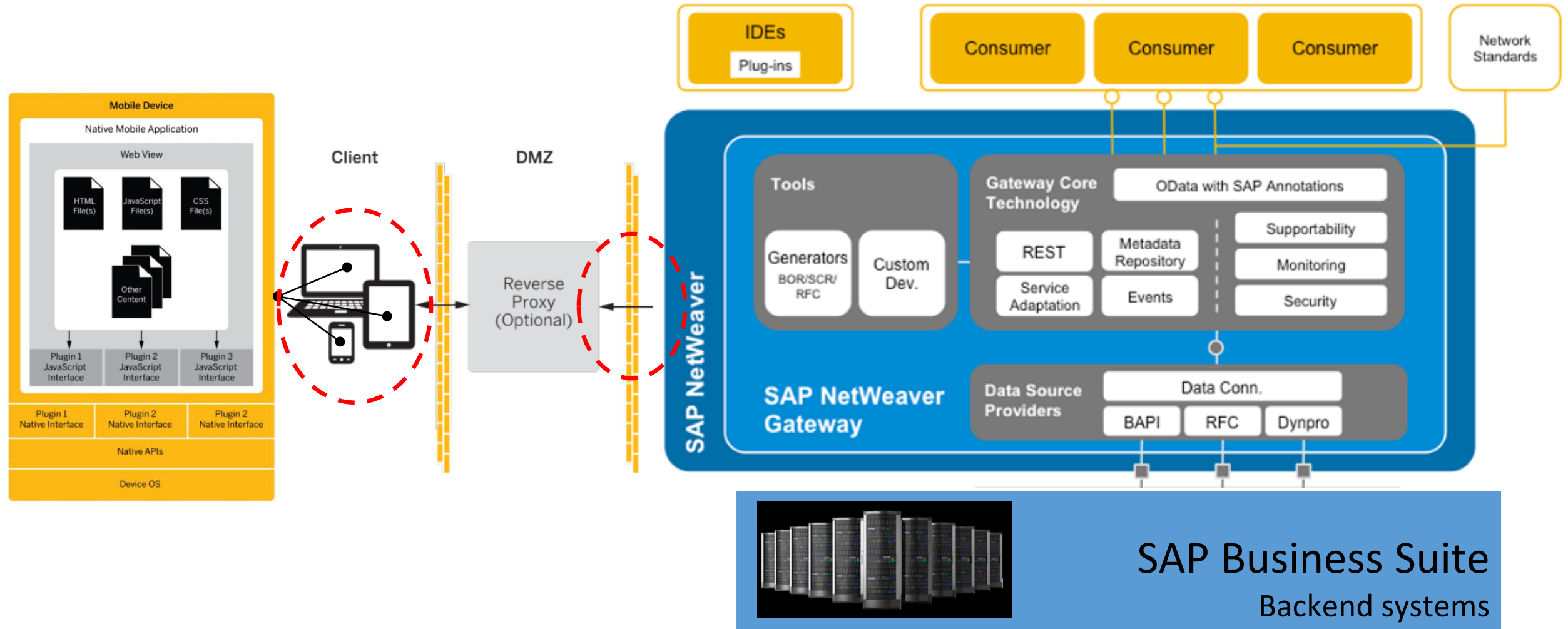
- Javascript + Native Code

AppUpdate	Push
Logon	Encrypted Storage
AuthProxy	Settings
Logger	ClientHub



Security challenges while building our application

1. Login mechanisms



1. Login mechanisms

- Anonymous Authentication

- No user/password needed
- No role mapping (generic users)

Use for public content

- HTTP Basic Authentication

- Defined at RFC7235
- User and password in plaintext (base64 encoded)

Without using SSL / TLS this method is totally useless



1. Login mechanisms

- Token-based Authentication

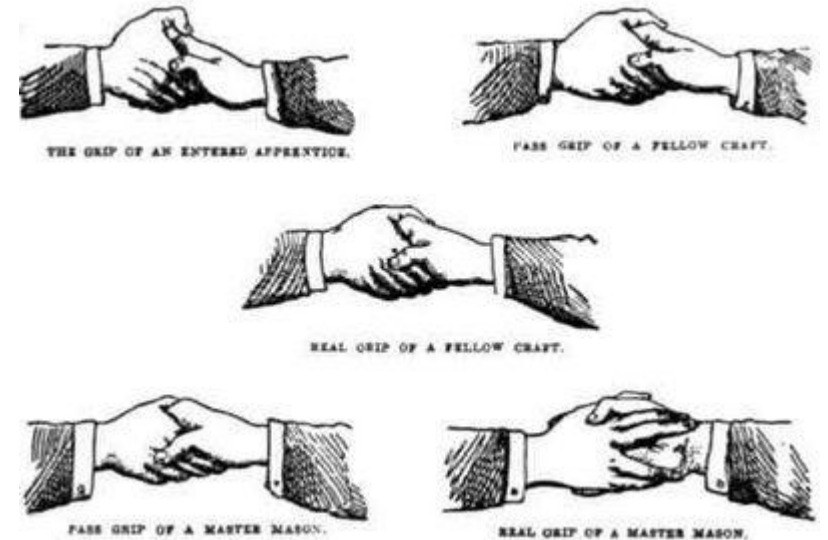
- Uses SAP Single Sign-On tokens
- In general it is used as an opaque value (as an HTTP Header)

Using SSL/TLS helps avoiding security issues

- Certificate-based Authentication

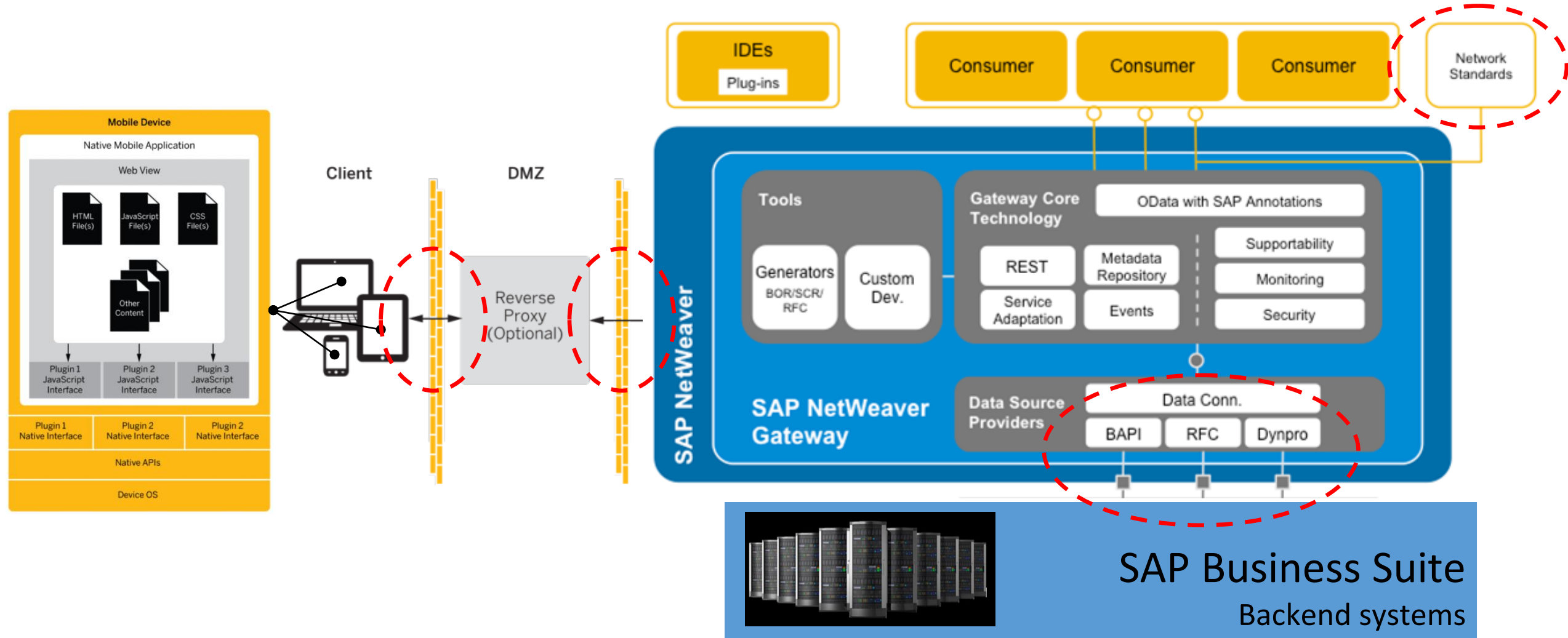
- Uses X.509 certificates
- Mutual authentication is assured

Not frequently used, due to it's complicated configuration



DEMO

2. Securing data in transit



2. Securing data in transit

- Use **HTTPS** as communication channel
- ..or a **VPN** network (or per app vpn)
- It **MUST** be used for every requested resource
- **DON'T** use Self Signed Certificates or suppress TLS error messages
- Using **Mutual Authentication** is highly recommended



2. Securing data in transit

Stay tuned with security updates related on securing communications.

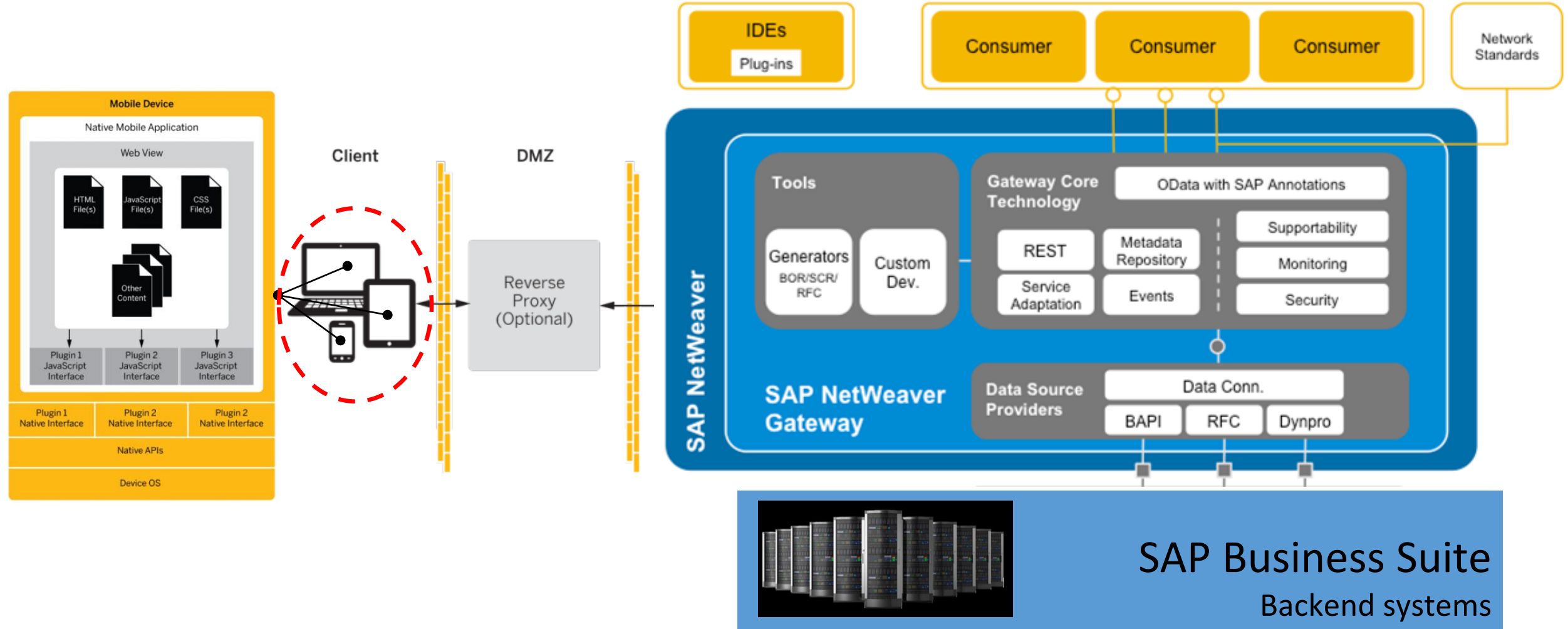
Notable SSL / TLS vulnerabilities recently found:

- Heartbleed (CVE-2014-0160)
- SMACKTLS
 - FREAK (CVE-2015-0204)
 - SKIP-TLS (CVE-2015-0205, CVE-2014-6593, ...)
- LogJam (CVE-2015-4000)

Also affects some VPN implementations



3. Securing data at rest



3. Securing data at rest

- Defining the proper data encryption requirements
 - Avoid custom "obfuscation"/encryption techniques
- **DON'T EVER** use hardcoded cryptographic keys in the app
 - Use the System Keyring if available
 - Use SAP ClientHub or similar
- Kapsel provides a plugin: **EncryptedStorage**
 - Sqlite / AES256
 - API based on the W3C Web Storage proposal
 - Or use SQLCipher...(https://www.zetetic.net/sqlcipher/)



DEMO

4. Patch Management



Componet	SAP Note	Short Title	Release Date
<i>SAP Afaria</i>	2153690	Multiple vulnerabilities in SAP Afaria Server	12.05.2015
	2155690	Missing authentication check in SAP Afaria	12.05.2015
	2132584	Buffer overflow in SAP Afaria 7 XcListener	10.03.2015
<i>Apache Cordova</i>	2116121	Hybrid Web Container 2.3.4.7320 vulnerable to XAS attack	10.03.2015
<i>SAP Mobile Platform</i>	2125513	XXE vulnerability in SAP Mobile Platform	10.03.2015
	2114316	Unauthorized use of application functions in SMP 3.0	10.02.2015
	2125358	SAP Mobile Platform XXE vulnarability	10.02.2015
<i>Sybase Unwired Platform</i>	2094830	Potential information disclosure relating to mobile onboarding	14.04.2015
<i>Agentry</i>	2036547	Security mitigation instructions for Agentry 6.1.3	09.09.2014
	2105793	Fixing Poodle SSLv3 vulnerability for Agentry	09.12.2014
	2038190	Potential information disclosure relating to the Agentry 6.1.3 iOS Client	09.12.2014

4. Patch Management



Componet	SAP Note	Short Title	Release Date
<i>SAP Afaria</i>	2153690	Multiple vulnerabilities in SAP Afaria Server	12.05.2015
	2155690	Missing authentication check in SAP Afaria	12.05.2015
	2132584	Buffer overflow in SAP Afaria 7 XcListener	10.03.2015
<i>Apache Cordova</i>	2116121	Hybrid Web Container 2.3.4.7320 vulnerable to XAS attack	10.03.2015
<i>SAP Mobile Platform</i>	2125513	XXE vulnerability in SAP Mobile Platform	10.03.2015
	2114316	Unauthorized use of application functions in SMP 3.0	10.02.2015
	2125358	SAP Mobile Platform XXE vulnarability	10.02.2015
<i>Sybase Unwired Platform</i>	2094830	Potential information disclosure relating to mobile onboarding	14.04.2015
<i>Agentry</i>	2036547	Security mitigation instructions for Agentry 6.1.3	09.09.2014
	2105793	Fixing Poodle SSLv3 vulnerability for Agentry	09.12.2014
	2038190	Potential information disclosure relating to the Agentry 6.1.3 iOS Client	09.12.2014

4. Patch Management



Componet	SAP Note	Short Title	Release Date
SAP Afaria	2153690	Multiple vulnerabilities in SAP Afaria Server	12.05.2015
	2155690	Missing authentication check in SAP Afaria	12.05.2015
Apache Cordova			10.03.2015
			10.03.2015
SAP Mobile Platform			10.03.2015
			10.02.2015
Sybase Unwired Platform			10.02.2015
			14.04.2015
Agentry	2036547	Security mitigation instructions for Agentry 6.1.3	09.09.2014
	2105793	Fixing Poodle SSLv3 vulnerability for Agentry	09.12.2014
	2038190	Potential information disclosure relating to the Agentry 6.1.3 iOS Client	09.12.2014

- Since September 2010, security notes are released the 2nd Tuesday of every month (SAP Security Patch Day)
- The notes information is only accessible to SAP customers
<https://service.sap.com/notes>
- Many security notes need to be applied manually
- Only the implementation of some Security Notes can be automatically analyzed using the transaction RSECNOTE

- 1. *Login mechanisms*
- 1. *Securing data in transit*
- 1. *Securing data at rest*
- 1. *Patch Management*



Conclusions

- Bring your own device (BYOD) is here to stay.
 - Building mobile applications integrated with SAP is challenging itself.
 - SAP i
 - In our appli
 - Our such least for a while..
- Use the Secure Sockets Layer (SSL/TLS) protocol in the SAP NetWeaver Gateway host to secure communication in your landscape.
 - Use Secure Network Communications (SNC) connections between the SAP NetWeaver Gateway host and the SAP systems.
 - The security guidelines described in the SAP NetWeaver Security Guide also apply to SAP NetWeaver Gateway components (as they are based on the same topology).
- In order to protect our business information, we need to protect **ALL** the systems and products within the landscape.



Questions?

Julian Rapisardi
jrapisardi@onapsis.com

Fernando Russ
fruss@onapsis.com

