SMP Security & Identity Management
An Introduction

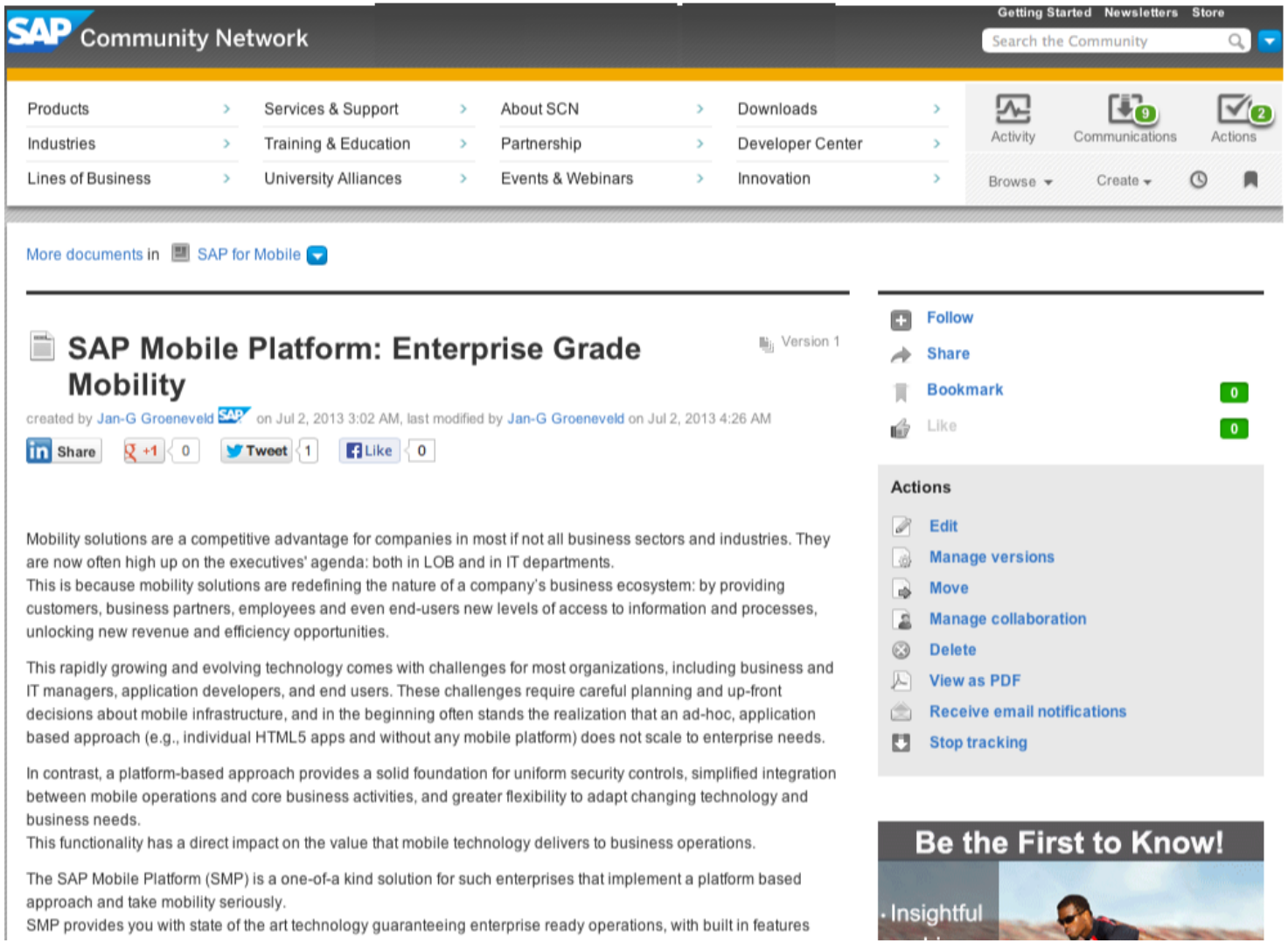
SMP Enterprise Grade Mobility – Webinar Series

Brought to you by the SAP Mobile Rapid Innovation Group (RIG)

SAP Mobile Platform: Enterprise Grade Mobility

On SCN pages and a series of webinars, we drill down into Enterprise Readiness aspects of the SAP Mobile Platform (SMP).

- On the **SCN Pages**, you find links to White Papers, How-To Guides, Blogs and other resources.
  http://scn.sap.com/docs/DOC-43424
- **Webinars** complement these published resources. The Webinar schedule is also published on SCN.
  http://scn.sap.com/docs/DOC-43425



Security & Identity Management - Introduction

SMP Enterprise Grade Mobility – Webinar Series
Dirk Olderdissen, Regional Mobility Presales, EMEA
July, 2013

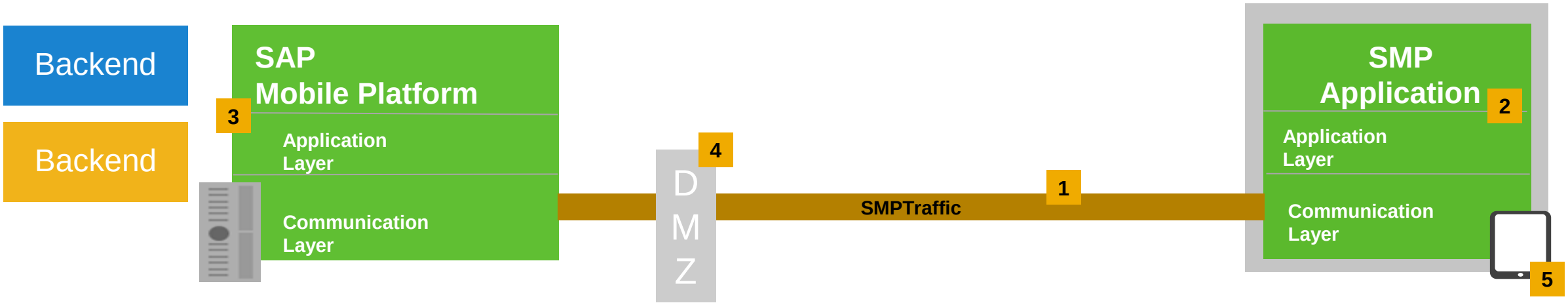
Agenda

1. SMP Security Overview
2. Transport Security
3. SMP Application Identification
4. Server Security Configuration
5. DMZ Security
6. Client Security

SMP Security Overview

Platform security elements

		SMP	SAP Afaria
1	Transport Security	X	
2	Application Security	X	X (partial)
3	Platform Security • Authentication • Backend Security	X	
4	DMZ Security	X	
5	Device Security		X



SMP Data transport encryption

The SMP client traffic can be encrypted.

- Most SMP protocols are actually already encrypted “out of the box”.
- When encryption is configured, the encryption is established before data is sent to the mobile device.
- The encryption type and details depend on the respective protocols that are being used.

SMP app ID check

SMP applications* need to present a valid app ID

- The app ID is created during the app enrolment process
- The app presents this ID on every connection with the SMP server
- The App ID is checked on the SMP server for validity
- The ID allows the SMP Server to uniquely identify each App on any particular device (for security + management + data handling)

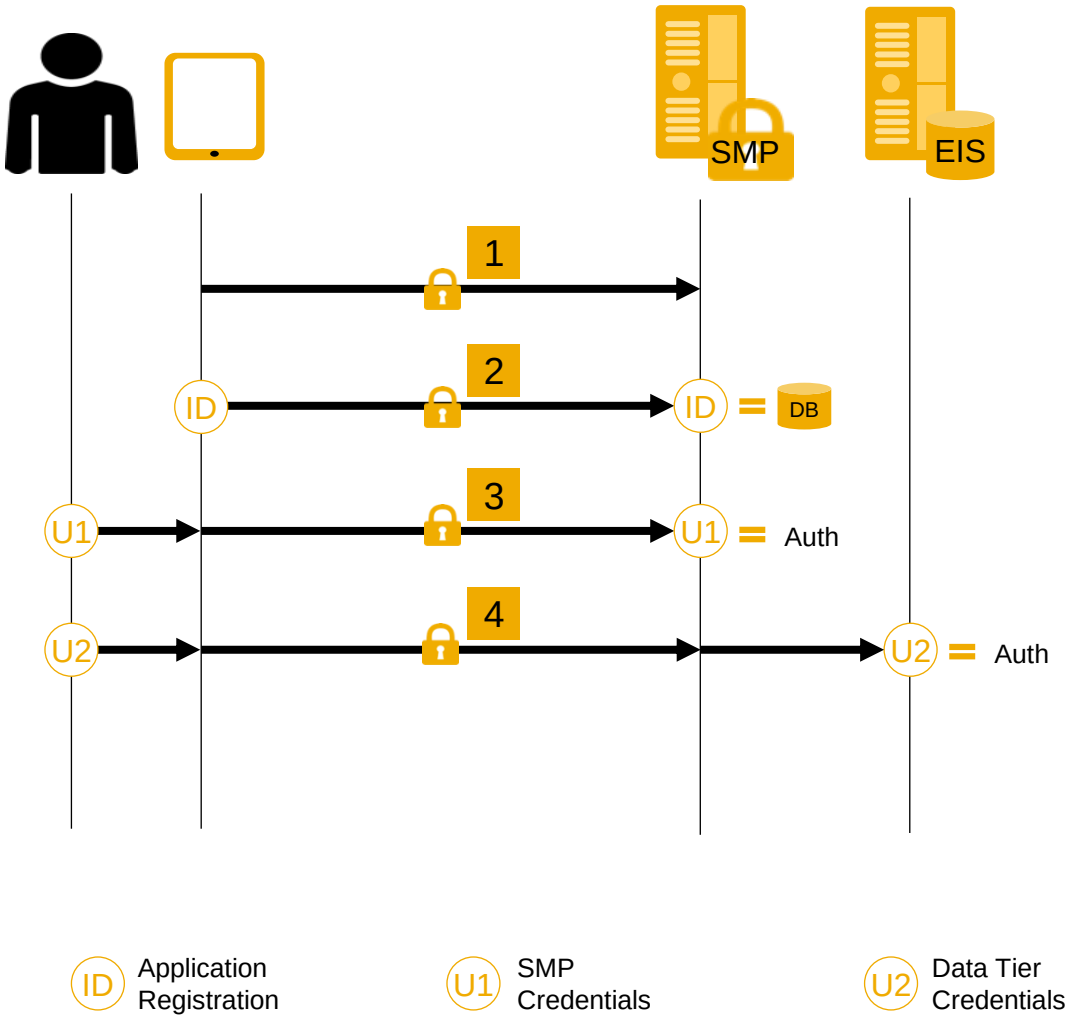
* HTTP Rest API – application connection ID is optional

Authentication

The app needs to authenticate against SMP and against the backend

- The app needs to present credentials for authentication
- The required credentials are configurable
- The authentication is a two tier authentication
  - First tier for SMP
  - Second tier for the Data Source

SMP communication process overview



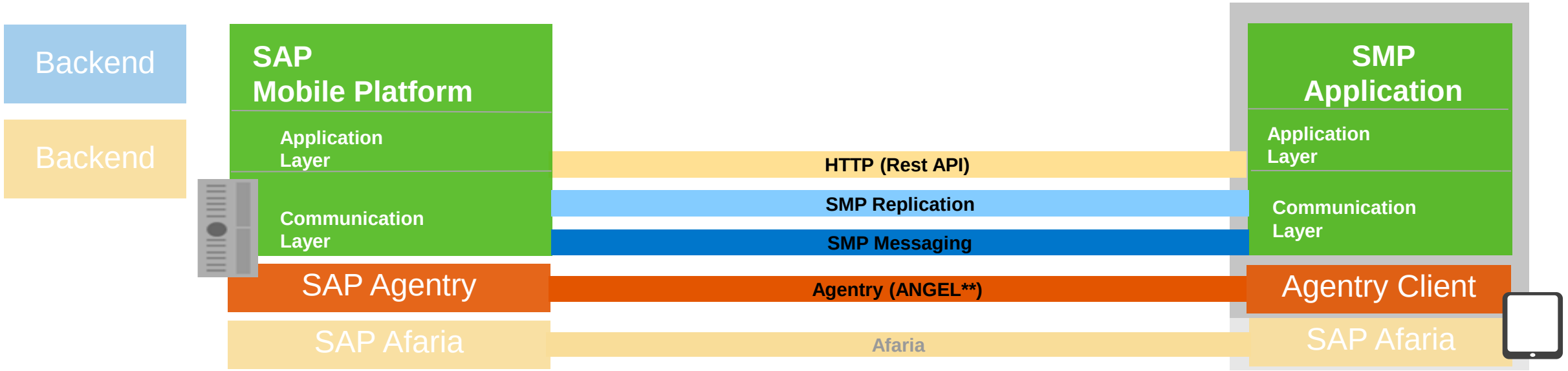
Steps taken before any data is sent to the mobile application

1. Transport Encryption is established when the client connects with SMP
2. Application registration (App ID) is verified
3. SMP server authentication takes place (first tier)
4. Data source (EIS) authentication takes place (second tier)

This process is different for SAP Agentry applications as of SMP 2.3

Protocols by platform version

	SUP 2.1.3	SUP 2.2	SMP 2.3	SMP 3.0*
SMP Messaging	X	X	X	X
SMP Replication	X	X	X	X
HTTP Rest API		X	X	X
SAP Agentry			X	X
SAP Afaria				



*SMP3.0 road map, subject to change, see disclaimer, **ANGEL – Agentry Next Generation Encryption

Transport Security

SMP Messaging communication

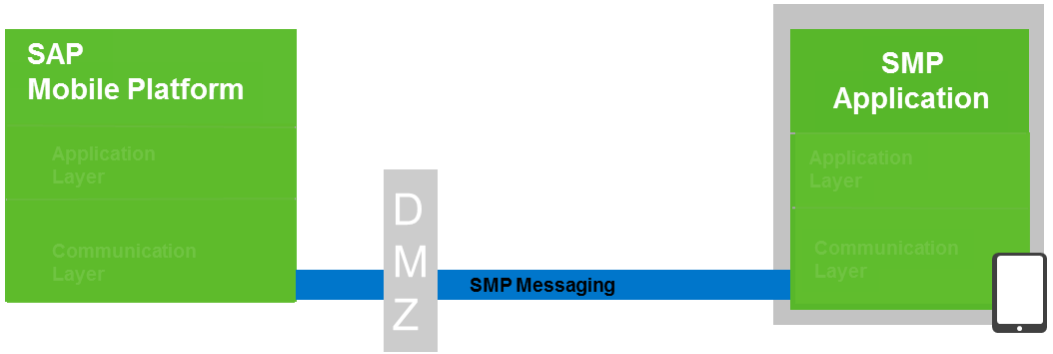
SMP Messaging is always compressed and encrypted

Protocol

- HTTP encapsulated (HTTPS is optional)
- Compressed & Encrypted Binary protocol

Encryption

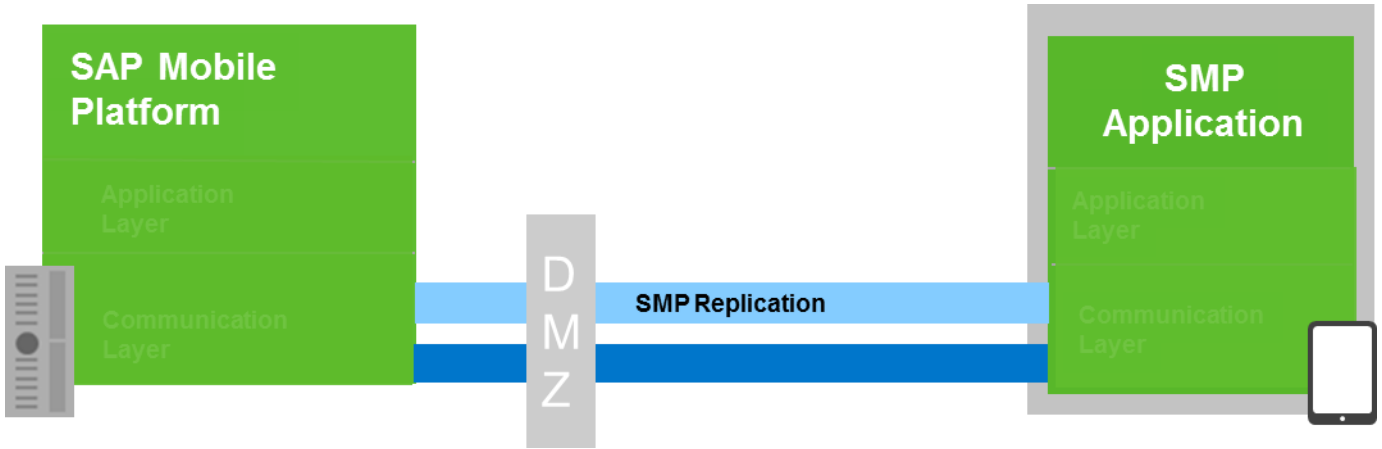
- 1024 bit asynchronous encryption
  - 1024 bit RSA Public Key exchange
- 128 bit AES synchronous encryption (payload)
  - Data traffic (payload) encryption from SMP-Client to the SMP-Server.
  - Synchronous keys are automatically renewed automatically during Synchronization Session.



SMP Replication traffic encryption

- **Replication traffic is encrypted with AES by default (SMP 2.1.3+)**
  - RSA for key exchange, 128bit AES transport encryption (configurable in SCC)
  - The RSA Public Key is transported to the SMP client via SMP Messaging
  - Traffic is HTTP with a binary payload, HTTPS encapsulation optional

- Devices need to be registered (via SMP Messaging) before data replication can take place
- SMP installs with default RSA keys – you MUST change them!

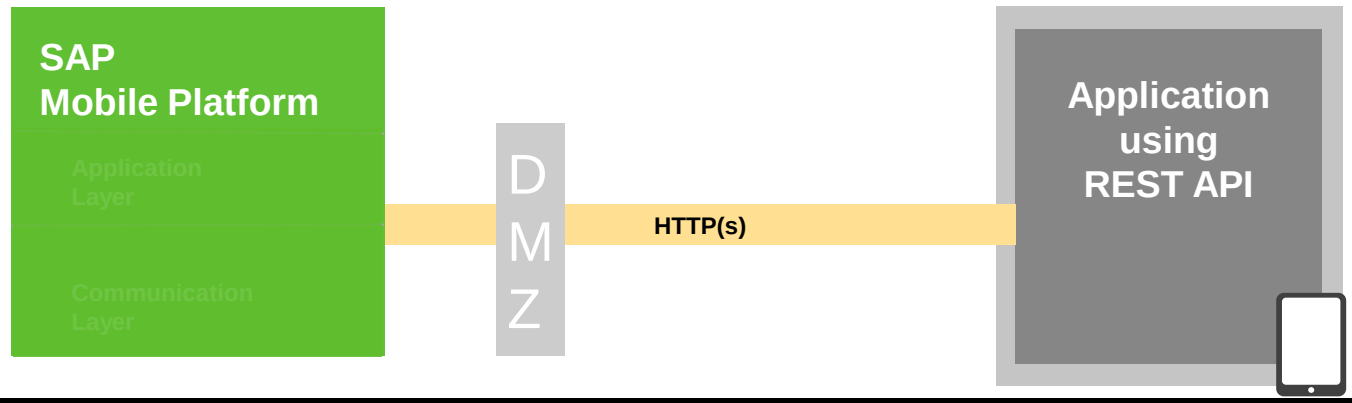


http://dcx.sybase.com/index.html#sup0213/en/com.sybase.infocenter.dc01703.0213/doc/html/aba1313418512005.html

HTTP REST API traffic encryption

The HTTP REST API is using regular HTTPS (SSL) for traffic encryption.

- REST API is a server side only API, no client side SMP specific modules
- HTTPS security level (SSL version), depends on the SSL Endpoint and the client implementation.
- The SSL for REST API traffic is often terminated on a customers reverse proxy or the SMP Relay Server.



SAP Agentry

SAP Agentry traffic can be encrypted with SSL

- The Agentry server is either stand-alone or part of SMP (v2.3 and higher), depending on the SMP version.
- The Agentry traffic protocol is called ANGEL, and is custom TCP binary traffic.

The Agentry Server is not (as of SMP 2.3) integrated into the SMP Security concept. All discussed concepts in this presentation do NOT apply to SAP Syclo Agentry if not explicitly stated otherwise.

SMP Application Identification

Application identification concept

In order for SMP to function properly and to supply a high level of security, every app needs to be uniquely identified.

A valid app identifier is used for

- **App security** – only apps with a valid app connection ID are legitimate. Combined with the user credentials (U) this is an ownership (ID) & knowledge (U) security concept
- **Data Synchronization and consistency** – required to sync the correct data differentials
- **App management** – allows a clear management and reporting of all apps, versions, devices and users

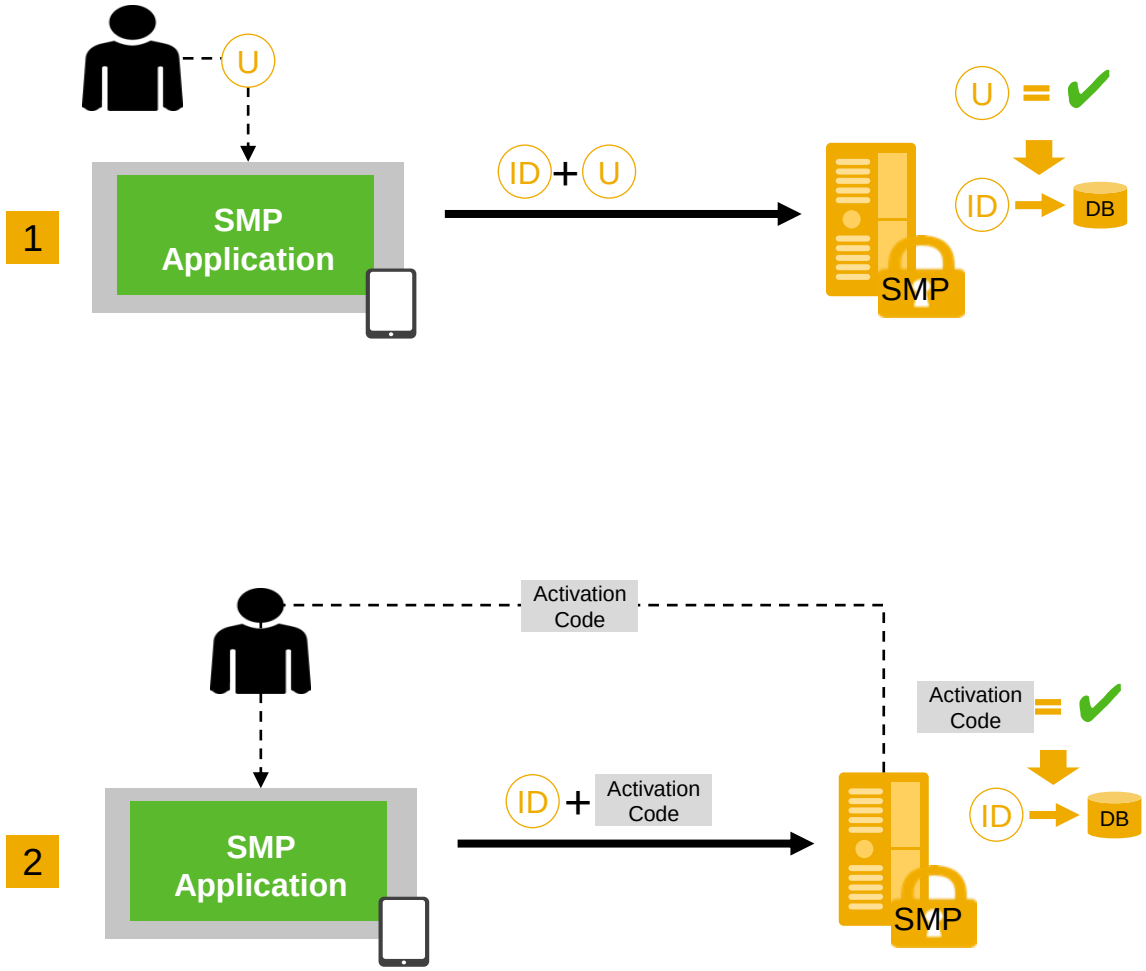
SMP App Registration

The SMP server needs to know the App connection ID – getting to know this ID is called the registration process

The registration process (part of enrolment) is protected, as only legitimate apps are supposed to register with the SMP server. This registration protection can be configured with SMP

1. **Credentials (configured authentication provider, automatic registration)**

2. **One time activation code (activation code is entered on app)**



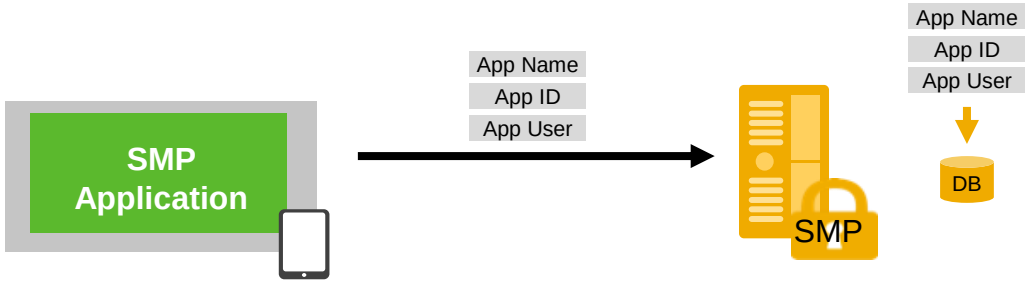
* HTTP Rest API – application connection ID is optional

SMP registration process details

During the registration, the SMP server combines three values into a fixed registration triple*

- **Application Name**
  SMP application name that the developer has defined during design time.
- **App connection ID**
  The unique ID for this particular application registration (usually hardware specific)
- **App user name**
  A name needed for administrative reference.

If this triple changes, the registration is considered invalid and the app needs to re-register.



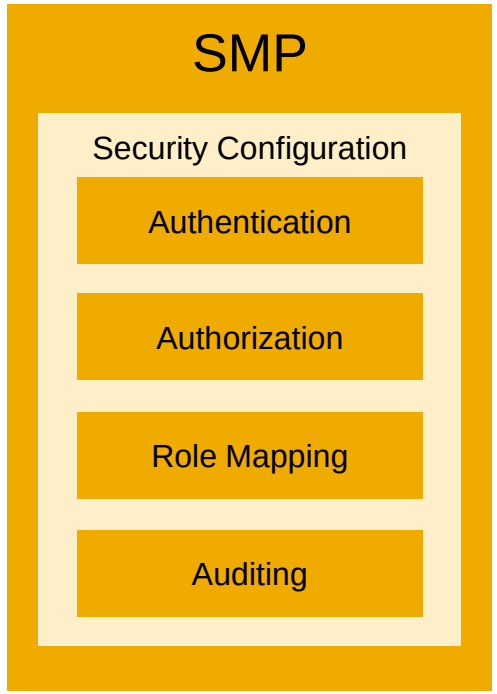
* HTTP Rest API – application connection ID is optional

Server Security Configuration

SMP - Authentication/Authorization

SMP utilizes the Common Security Infrastructure (CSI)

- **Authentication** – making sure the connecting user is who he claims to be
- **Authorization** – check where the user belongs to and if he is entitled or not
- **Role Mapping** – Puts the user into a SMP definable Role for easier administration
- **Audit** – logging of authentication/authorization decisions made SMP (off by default)

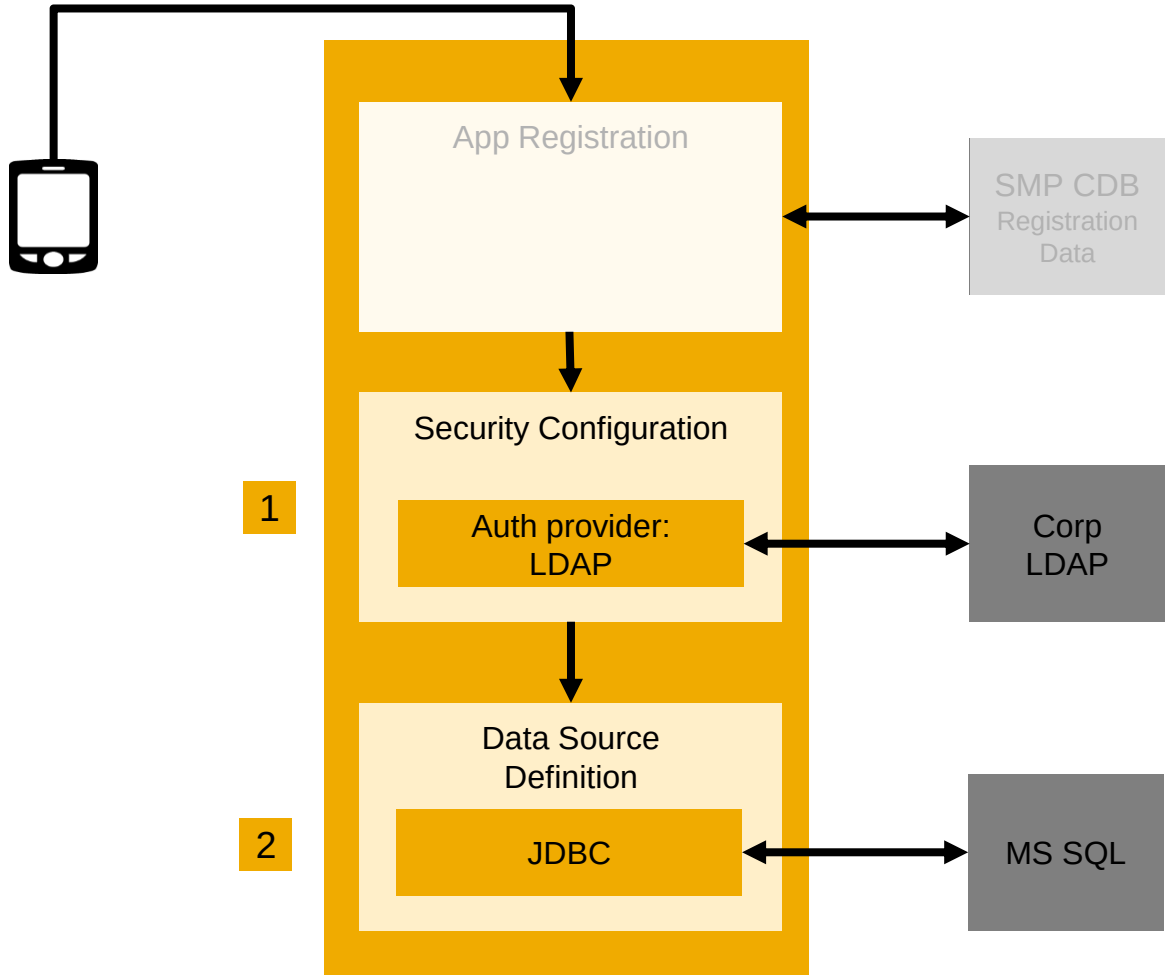


http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01703.0213/doc/html/aba1313092289408.html

SMP authentication

The SMP authentication is a two step (tier) process:

1. **SMP Server authentication -** configurable, using SMP authentication providers
2. **Data Source authentication -** depends on data source



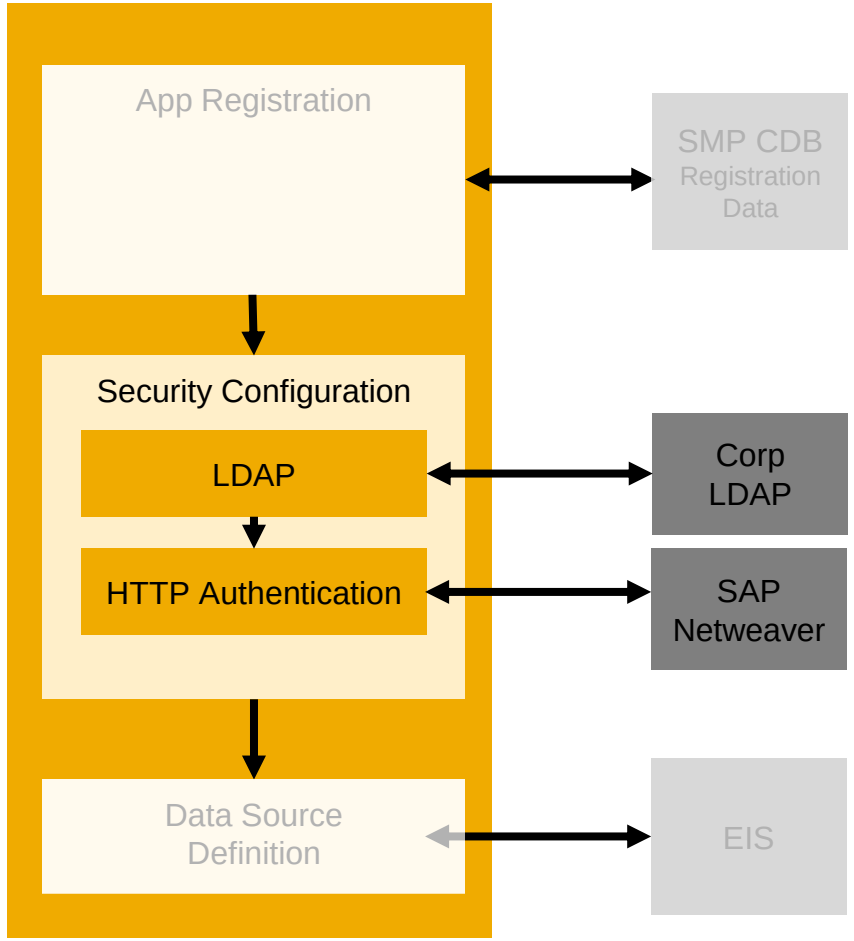
SMP Authentication Providers

SMP provides different authentication providers* that can be used in the Security Configurations (as of SMP2.3)

- NoSecurity
- LDAP
- NTProxy
- SAP SSO Token
- Certificate Authorization
- Certificate Validation
- User Role Authorizer
- HTTP Authentication
- Custom

Authentication providers can also be combined*

- E.g. Use LDAP for authentication and HTTPAuth to generate a SSO2 token



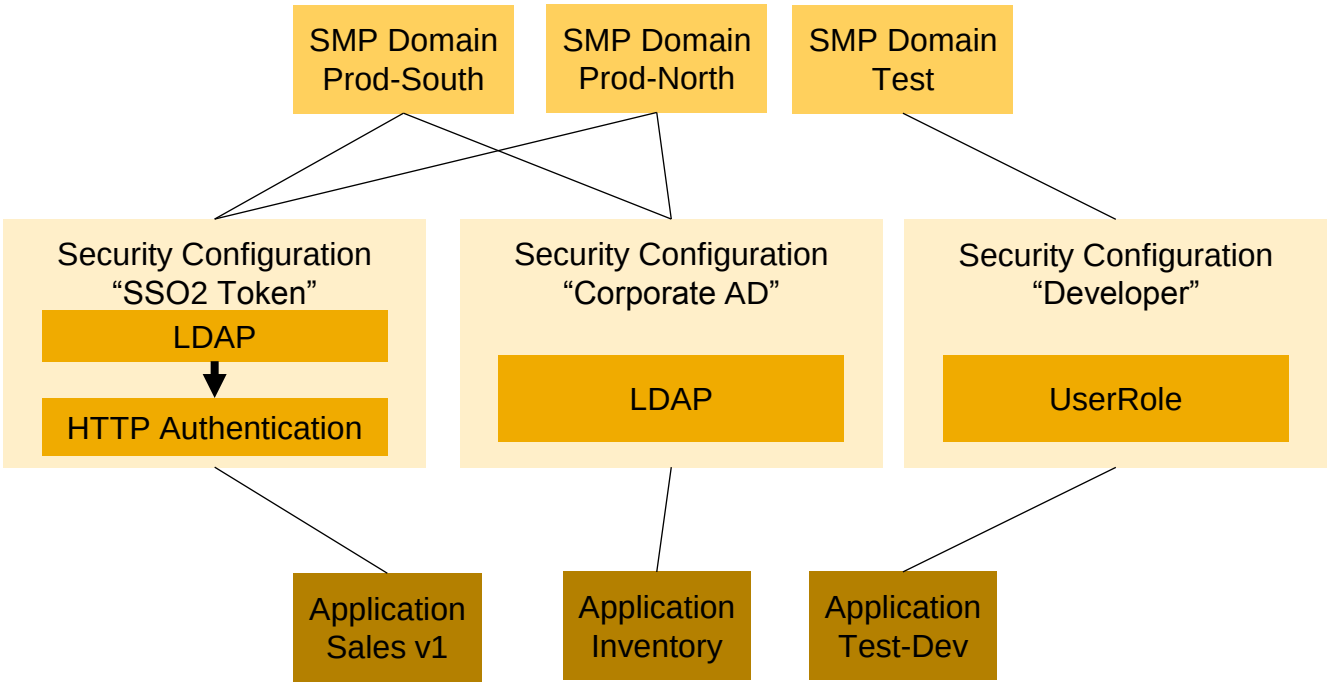
*http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc01930.0230/doc/html/aba1253113891962.html

** http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01930.0230/doc/html/asc1229700941188.html

SMP Security Configurations

SMP Security configurations are defined globally and can then be assigned to

- SMP domains (tenants)
- Applications (application templates)
- Packages (data structure definitions)

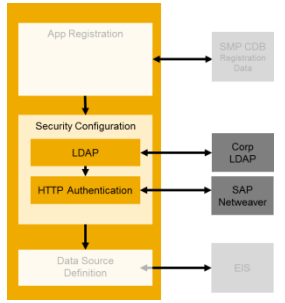


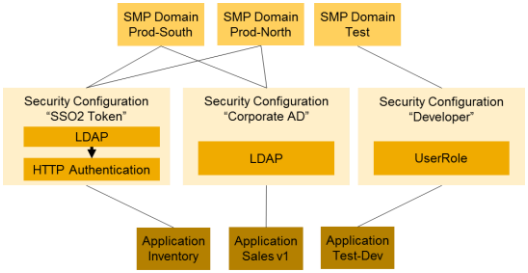
*http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01930.0230/doc/html/aba1313092288033.html

Value

By providing these security configuration features, the SAP Mobile Platform allows:

- Implementation of complex security requirements (e.g. SSO with SAP tokens, Network Edge Authentication, …).
- Custom authenticators if required.
- Multi-Tenant support for large corporations.
- Global security configurations can be done by security experts and then used and assigned by SMP administrators.
- Multiple apps can share a security configuration without the need of re-wirering for each app.
- …





DMZ Security

SMP Protocol Reference

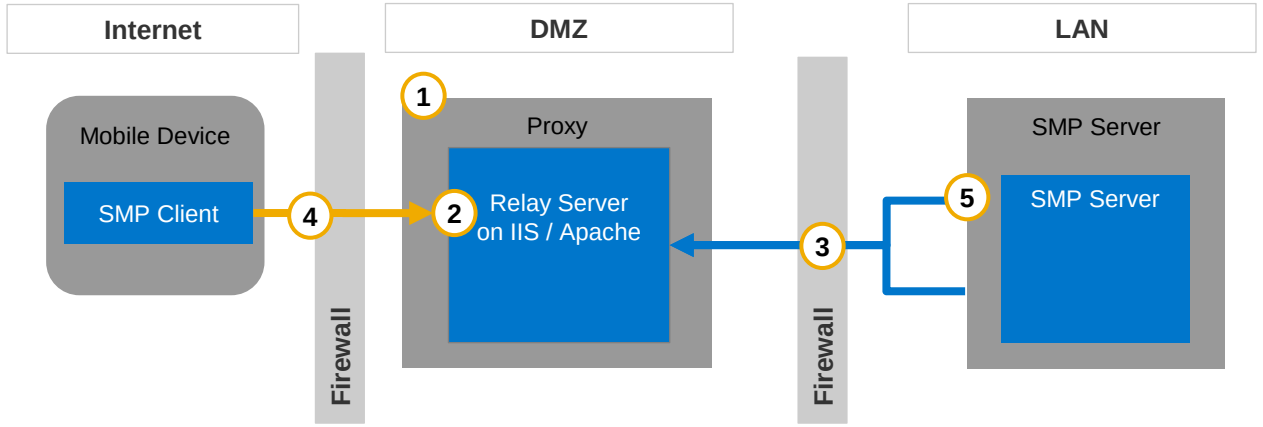
SMP is utilizing some very specialized protocols. In order to find the best suited networking setup, the used protocols and their individual nature needs to be kept in mind.

Protocol	Comment	Structure	HTTPS	Relay Server support	Out-of-the-box Reverse Proxy filters
Messaging	aka – iMO, MOCCA, MBS, ODP traffic	HTTP, plaintext header with binary body,	Yes, HTTPS encapsulation optional	Yes	No
Replication	aka - Mobilink, RBS	HTTP, binary payload,	Yes, HTTPS encapsulation optional	Yes	No
HTTP REST	HTTP standard	HTTP plain	Yes, HTTPS optional	Yes	Yes
ANGEL	Syclo Agentry traffic	TCP binary, SSL encrypted	No	No	No

SMP Relay Server

RelayServer (RS) is an optional DMZ security component

1. Additional network security component in front of SMP
   - Prevents a direct connection from the internet to the SMP server
2. Allows only SMP / Afaria Traffic, all other traffic is dropped / blocked (basic protocol checks)
3. Requires only one outbound port in the inner DMZ (messaging & replication & Rest API)
4. Allows to reduce the open inbound ports from the internet, e.g. reduction to 443 for SMP traffic.
5. Provides built in load balancing for SMP & Afaria clusters (built in round robin)



Relay Server FAQ

1. **Is the Relay Server required?**
   - Use of the Relay Server is considered best practice for security and architecture improvements.
   - Technically, the RS is not required, but adds some security and architectural benefits that a reverse proxy usually does not provide.
2. **Can I use a reverse proxy instead of the Relay Server?**
   - Technically this is possible, but not recommended.
   - Due to the nature of many SMP protocols, reverse proxies are
     - very hard to configure if they are to provide a security benefit
     - SAP support can not help as this is a customer specific infrastructure
     - Unless you know what you do, potentially less secure as the RS
3. **Do I need to license the Relay Server?**
   - No, the Relay Server is part of the SMP and does not need to be licensed separately.
4. **Are there any exceptions?**
   - Yes, using the RS is a customer individual decision. e.g. when using Network Edge Authentication, RS may be considered redundant.

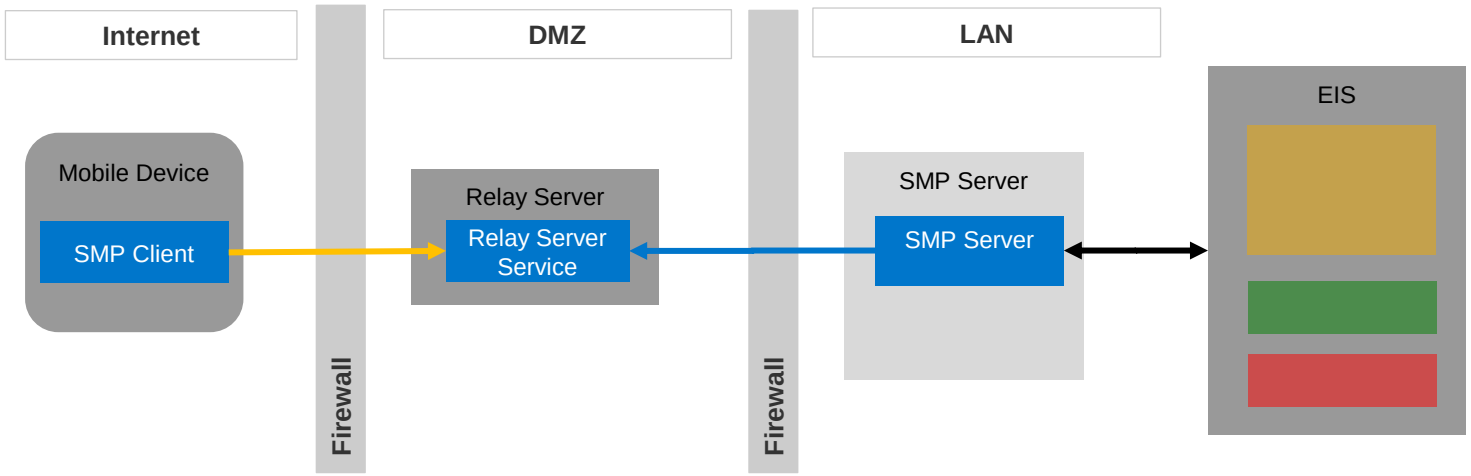
SMP Network Setup Examples - Regular

Major denominators

1. Most common architecture with RS in DMZ

Comments

- Best known setup by tech support, consulting and eco-system
- Best covered by product and supporting documentation



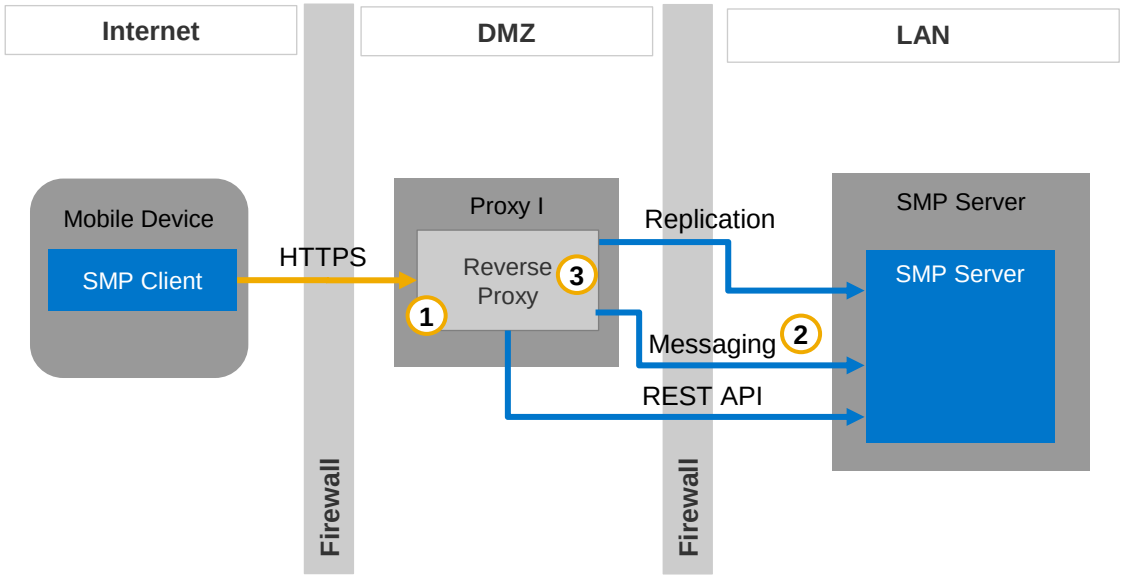
SMP Network Setup Examples
- SMP landscape only with Reverse Proxy (no RS)

Major denominators

1. Reverse Proxy as HTTPS endpoint
2. Traffic routing rules needed
3. Custom protocol filters or TCP pass-through required

Comments

- Reverse Proxy can't filter SMP protocols out of the box – custom filters required
- No outbound port model
- Network Edge authentication recommended



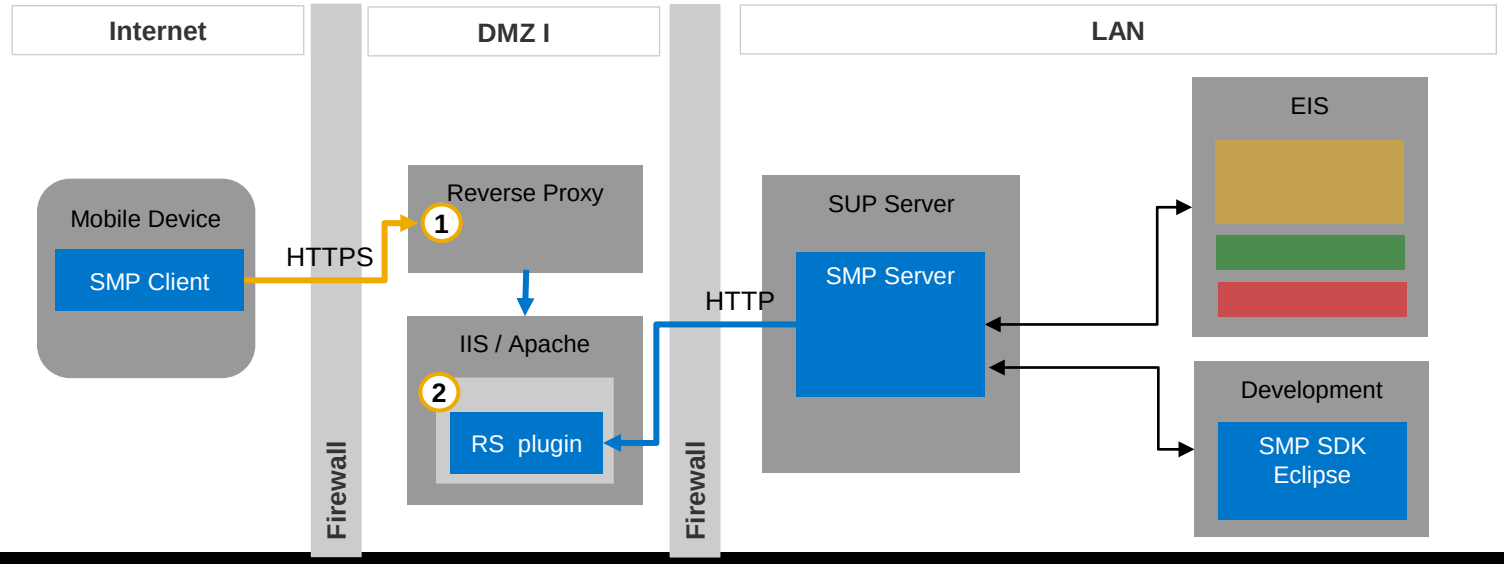
SMP Network Setup Examples - Reverse Proxy and RS

Major denominators

1. Reverse Proxy as HTTPS endpoint
2. RelayServer for additional security and ease of routing

Comments

- Reverse Proxy for corporate security policy compliance
- Maintaining communication benefits of RS (outbound port, single port)
- No traffic routing rules needed on Reverse Proxy

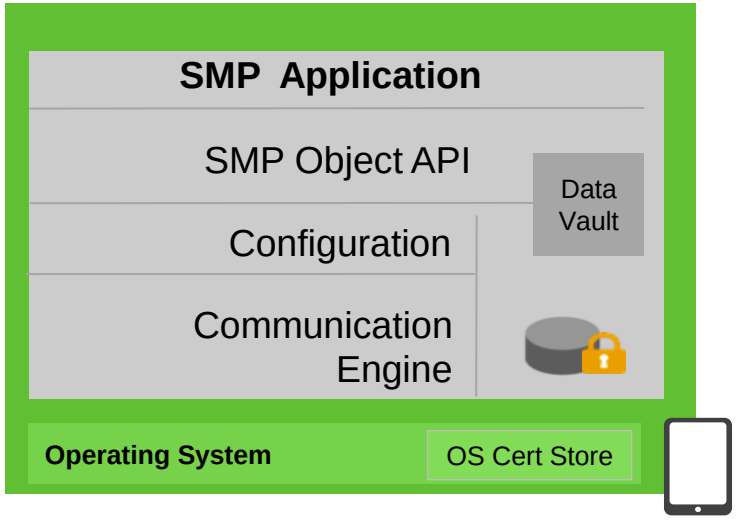


Client Security

Database Encryption

SMP mobile database can be encrypted with 256 bit AES.

- SMP Object API provides methods to generate a secure-random AES (256bit) key and encrypt the local DB with it.
- The app developer has all the tools to implement good data security on the mobile device
  - Create key
  - Encrypt DB
  - Store key securely (Data Vault)

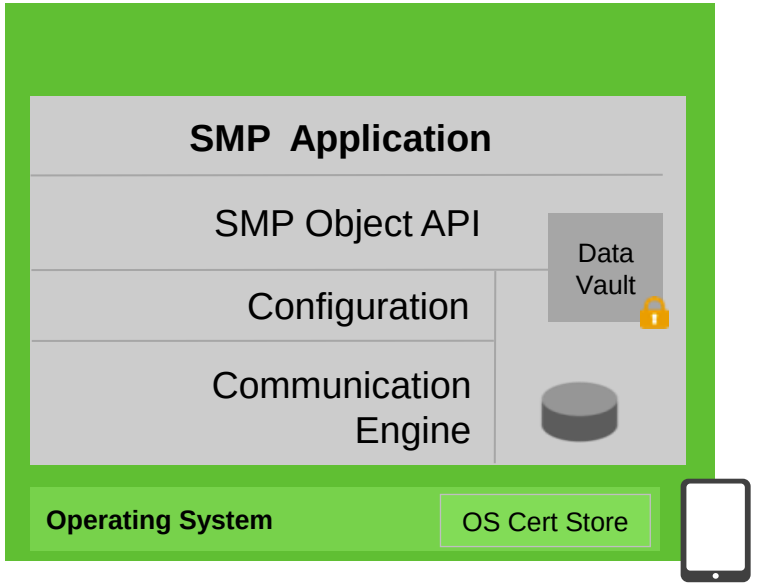


http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01703.0213/doc/html/aba1253043651786.html

Data Vault
- Concept

The Data Vault provides encrypted storage of occasionally used, small pieces of data.

- **SMP native applications**
  - Object API that provides secure data storage on the mobile device
  - 256bit AES encrypted
  - Vault API is device agnostic
- **Usage**
  - Application queries user for password
  - Password is used (salted & hashed) to unlock Data Vault
  - Application can access secrets e.g.
    - DB encryption key
    - Backend access credentials

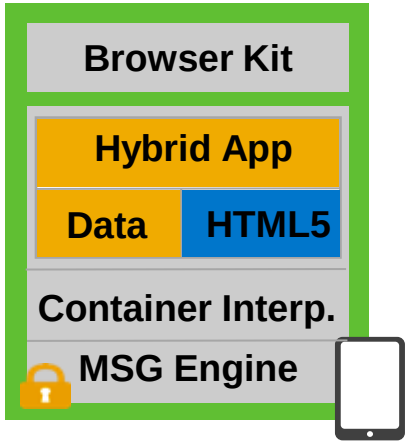


Taken from the Data Vault documenation: http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01703.0212/doc/html/aba1317138682352.html

Hybrid Web Container
- Container security benefits

The HWC provides built in cross platform security

- Local Data Security
  - Data at rest encryption.
  - Encrypted offline storage available
  - Browser Kit is used (not the device browser) prevents exposing data via browser cache, history or offline storage.
- Communication Security
  - SMP Server communication is encrypted.
  - Built in app-device ID association
- Backend Security
  - SMP platform authentication & authorization concepts apply (e.g. support for SSO).
  - SMP data source management for user data source access management etc.
  - User and application management

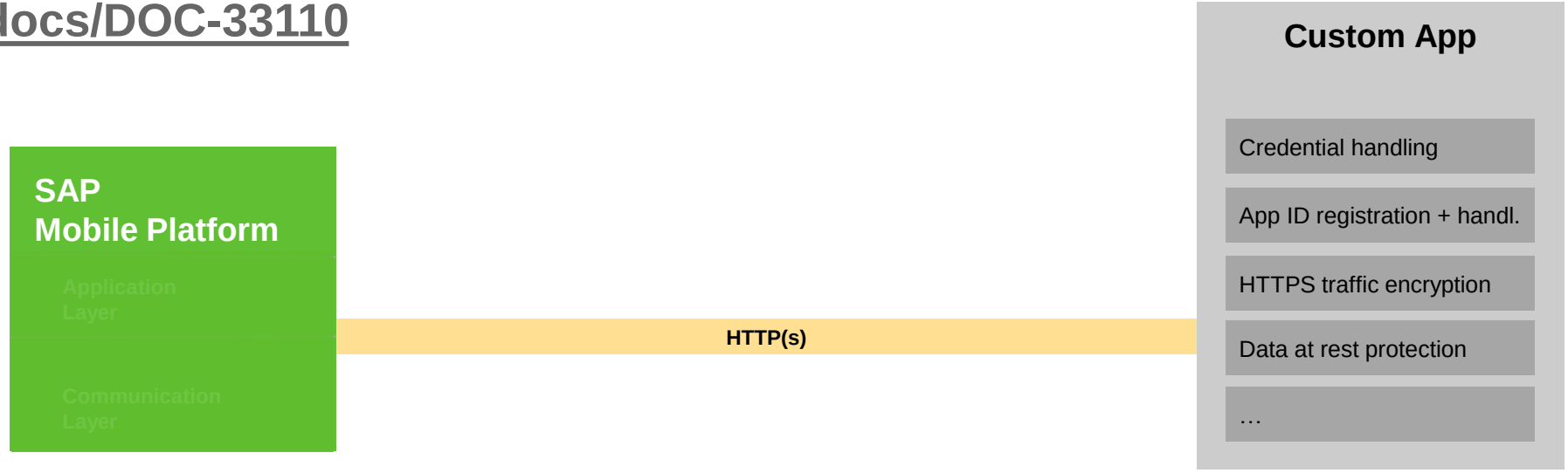


Rest API client security

The SMP Rest API is a server side API only. That means the application developer has to handle client side security all by himself with his available developer tooling, as of SMP 2.3.

The SAP Mobile Platform road map has plans to provide great tooling to increase developer productivity. E.g. Mobile Application Framework (MAF), Application Builder, etc.

Product road maps can be found here:
http://scn.sap.com/docs/DOC-33110



Wrapup

Wrapup

This presentation is the first part of a planned series of 4 SMP security webcasts. Lookout for the other three parts, currently targeted for October/November 2013.

Webinar recordings and announcements can be found here
http://scn.sap.com/docs/DOC-43425

SMP security content starting point on SCN
http://scn.sap.com/docs/DOC-44251

SMP documentation security starting point
http://infocenter.sybase.com/help/topic/com.sybase.infocenter.dc01930.0230/doc/html/title.html

Thank you

Contact information:

Dirk Olderdissen
Solution Advisor, Regional Mobility Presales, EMEA
dirk.olderdissen@sap.com

© 2013 SAP AG. All rights reserved.

© 2013 SAP AG. Alle Rechte vorbehalten.