experience success

simplify experience | harness data | stay ahead | be efficient

Charter Security High Level Solution

Ron Gal

Security Architect

June 2015

Information Security Level 2 – Sensitive

amdocs

embrace challenge experience success

Agenda

- Introduction & Solution Overview
- Application Security
- Infrastructure Security
- Roles and Responsibilities
- Compliance Matrix Review
- Q&A

Agenda

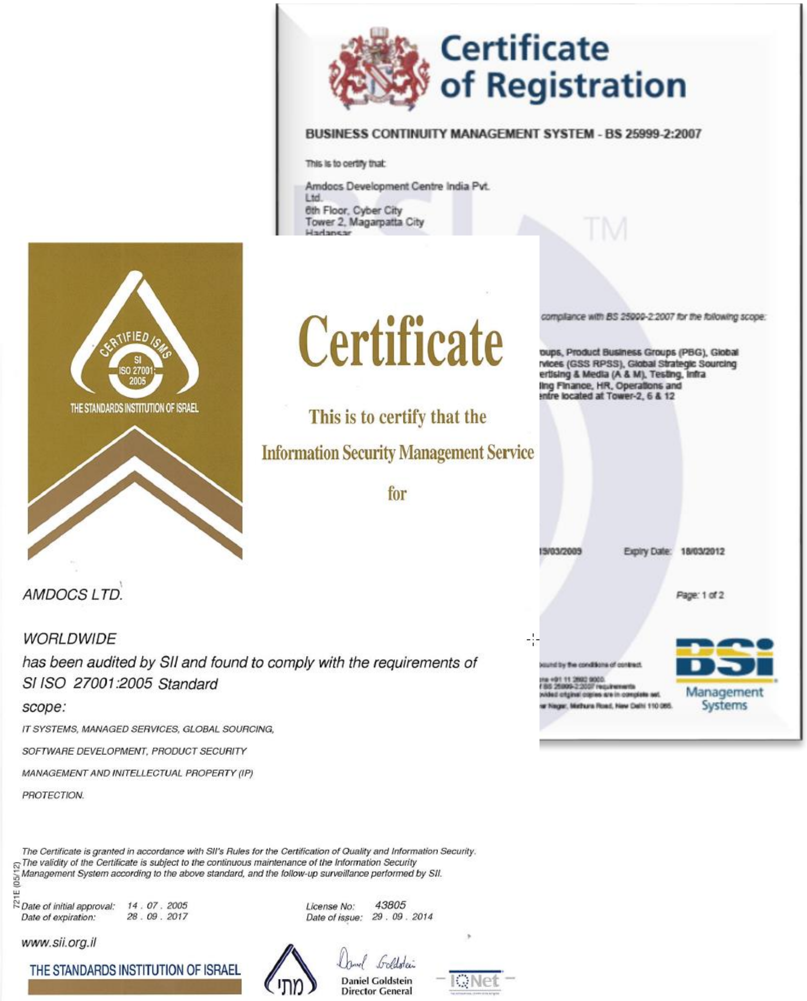
- **Introduction & Solution Overview**
  - Introduction
  - Amdocs SDLC
  - Security Solution Overview
  - Amdocs Security Manager (ASM) Overview
- Application Security
- Infrastructure Security
- Roles and Responsibilities
- Compliance Matrix Review
- Q&A

Introduction

- Ron Gal – Security Architect
  - Over 14 years of experience as Information Security Professional
  - Expertise in product security domain
  - Extensive knowledge security methodology
  - Managing security designs for various customers
  - Lead the security architecture team of the Amdocs Delivery unit

Amdocs SDLC

- ISO 27001 Certified
  - Policies and Procedures
  - Security Awareness & Education
  - Secure Development Life Cycle
- BS25999 Certified
- COBIT Maturity 4.2 (At the end of 2011 By Deloitte)
- Dozens of certified security experts (CISSP, CRISC, CEH…)



Certificate
of Registration

BUSINESS CONTINUITY MANAGEMENT SYSTEM - BS 25999-2:2007

This is to certify that:

Amdocs Development Centre India Pvt.
Ltd.
6th Floor, Cyber City
Tower 2, Magarpatta City
Hadapsar

compliance with BS 25999-2:2007 for the following scope:

oups, Product Business Groups (PBG), Global
rvices (GSS RPSS), Global Strategic Sourcing
ertising & Media (A & M), Testing, Infra
ling Finance, HR, Operations and
entre located at Tower-2, 6 & 12

15/03/2009 Expiry Date: 18/03/2012

Page: 1 of 2

bound by the conditions of contract.
ne +91 11 2692 9000.
f BS 25999-2:2007 requirements
vided original copies are in complete set.
ar Nagar, Mathura Road, New Delhi 110 065.

BSi
Management
Systems

CERTIFIED ISMS
SI
ISO 27001
2005
THE STANDARDS INSTITUTION OF ISRAEL

Certificate

This is to certify that the

Information Security Management Service

for

AMDOCS LTD.

WORLDWIDE
has been audited by SII and found to comply with the requirements of
SI ISO 27001:2005 Standard
scope:

IT SYSTEMS, MANAGED SERVICES, GLOBAL SOURCING,

SOFTWARE DEVELOPMENT, PRODUCT SECURITY

MANAGEMENT AND INITELLECTUAL PROPERTY (IP)

PROTECTION.

The Certificate is granted in accordance with SII's Rules for the Certification of Quality and Information Security.
The validity of the Certificate is subject to the continuous maintenance of the Information Security
Management System according to the above standard, and the follow-up surveillance performed by SII.

721E (05/12)

Date of initial approval:	14 . 07 . 2005	License No:	43805
Date of expiration:	28 . 09 . 2017	Date of issue:	29 . 09 . 2014

www.sii.org.il

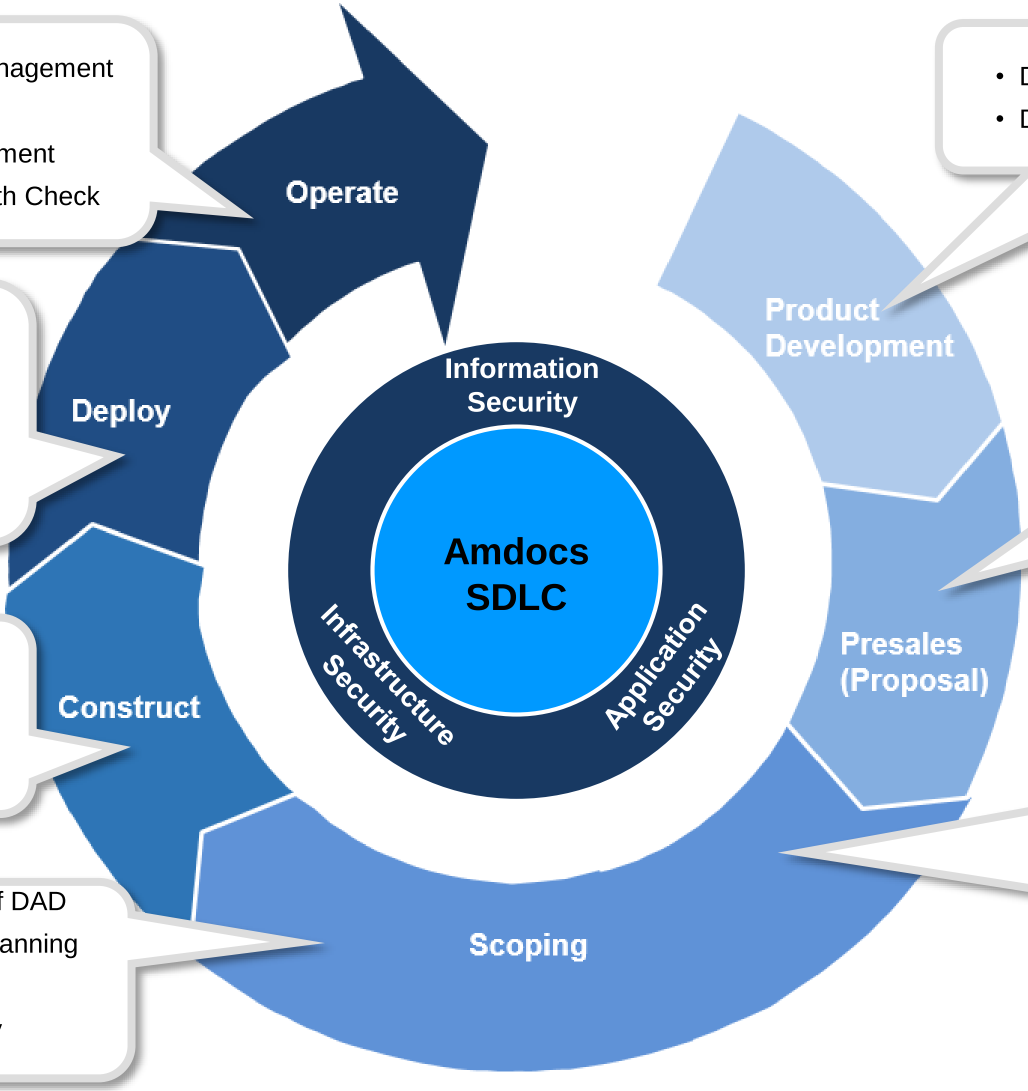
THE STANDARDS INSTITUTION OF ISRAEL

מתי

Daniel Goldstein
Daniel Goldstein
Director General

IQNet

Amdocs Secure Development Life Cycle (SDLC)



- Threat & Vulnerability Management
- Security monitoring
- Security incident management
- Information Security Health Check

- Security cleanup as part of packaging
- Secure Implementation Securing data during conversion & migration
- Penetration Testing as part of UAT

- Secured design / coding
- Security Testing
- Implement security roles & profiles

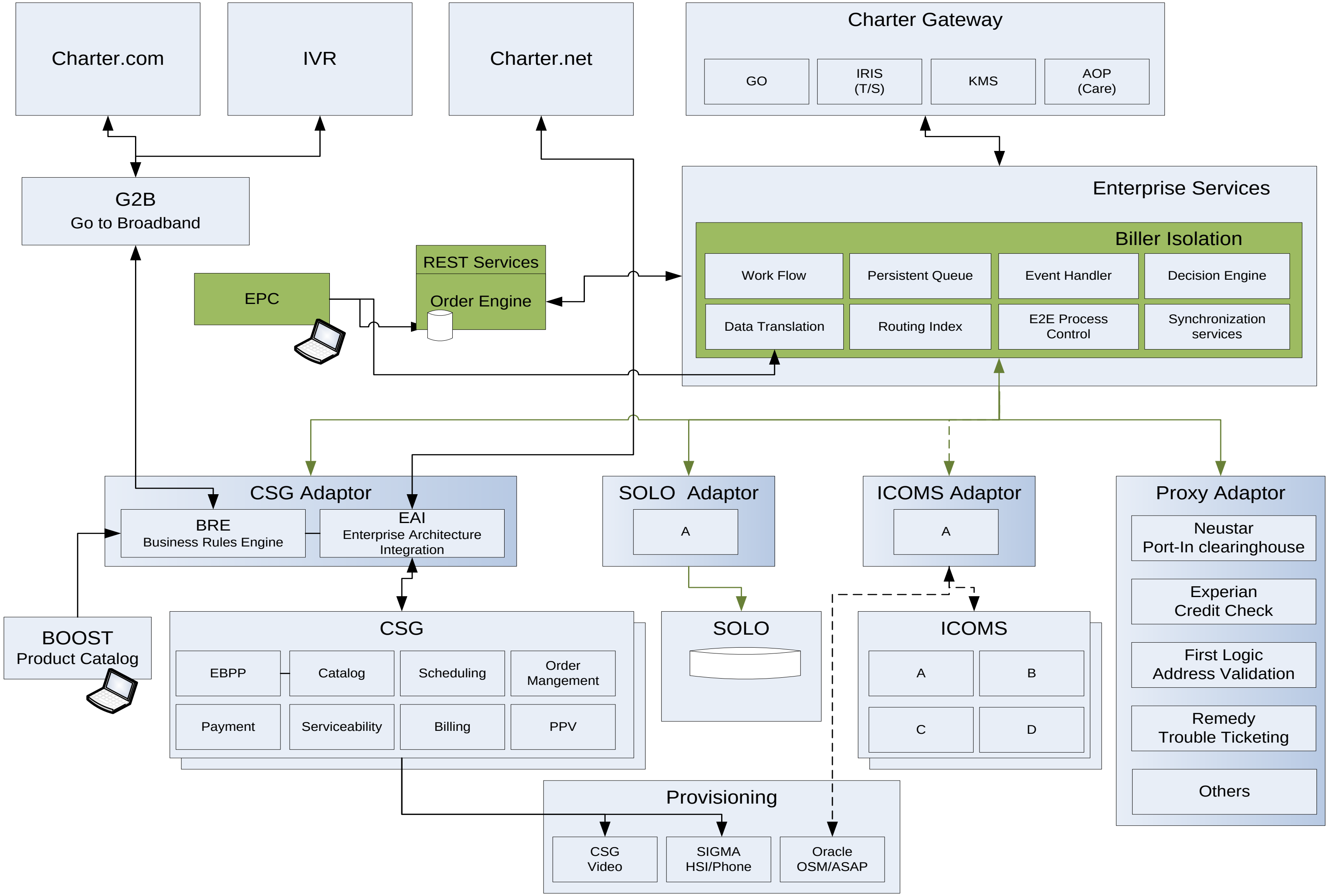
- Security as part of DAD
- Security testing planning
- Role engineering
- Technical security parameters

- Define non-functional requirements
- Design review input

- Answers to security questions (RFx)
- Customer engagements
- Contract review (legal)

- Define the system security high level solution
- Security requirements coverage in interface design
- Security CR Impact Analysis
- Security HLD signed off

Security Solution Overview
Security Solution Scope – Target Architecture



Security Solution Overview
Security Solution Scope – cont’

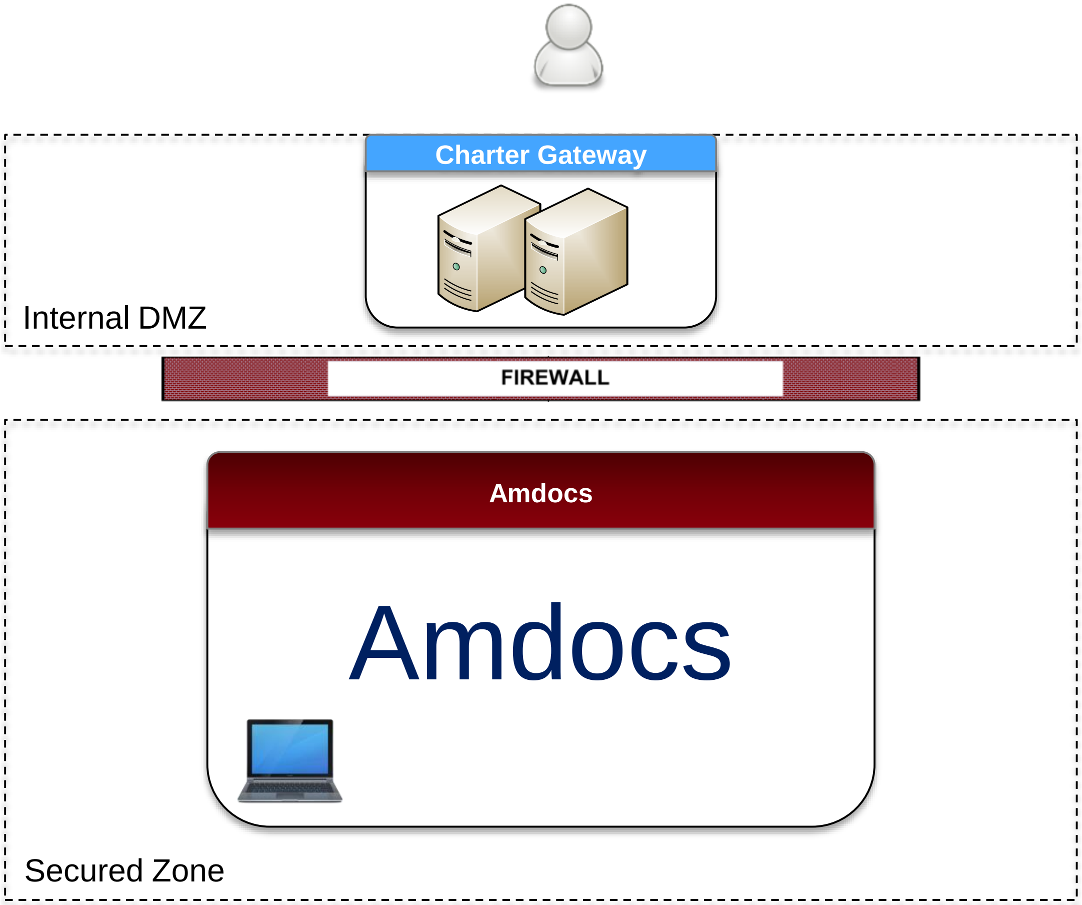
- MEC
- Ordering
  - Backend
  - REST services
- Biller Isolation
  - Search Engine
  - Operational UI
  - Web Services
- Reporting & BI
  - QlikView implementation

Security Solution Overview
Assumptions

- Operational security is under Charter's responsibility
- Charter Gateway will be the security gateway to the Biller Isolation layer
- Charter Gateway will be the security GW to the Ordering REST services
- Files read by Amdocs systems are subjected to customer security restrictions – anti-virus, size check, etc.

Solution Overview

Network Deployment Diagram – End State



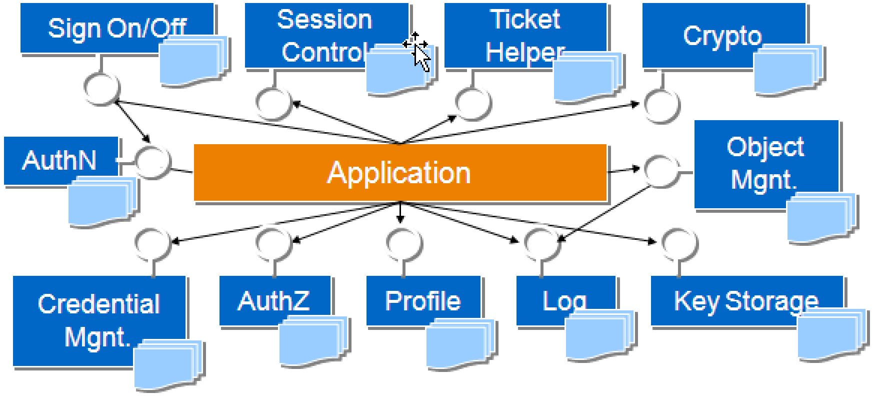
Solution Overview

Interface Types

- ***Graphical User Interfaces*** **(GUI)**
- ***Services***
  - ***Inbound*** – Services exposed by Amdocs system
  - ***Outbound*** – Services consumed by Amdocs system
- ***File*** – Data files extracted/processed by Amdocs system will reside in the secured zone

Amdocs Security Manager (ASM) Overview

- An application-level security framework used across the Amdocs portfolio, providing solid and robust protection of applications
- Based on "AAA" of Application Security:
  - **A**uthentication (including User Management)
  - **A**uthorization
  - **A**ccounting
- ASM comprises detachable modules accessible by the applications and other ASM modules
- An ASM library is deployed with the applications



Agenda

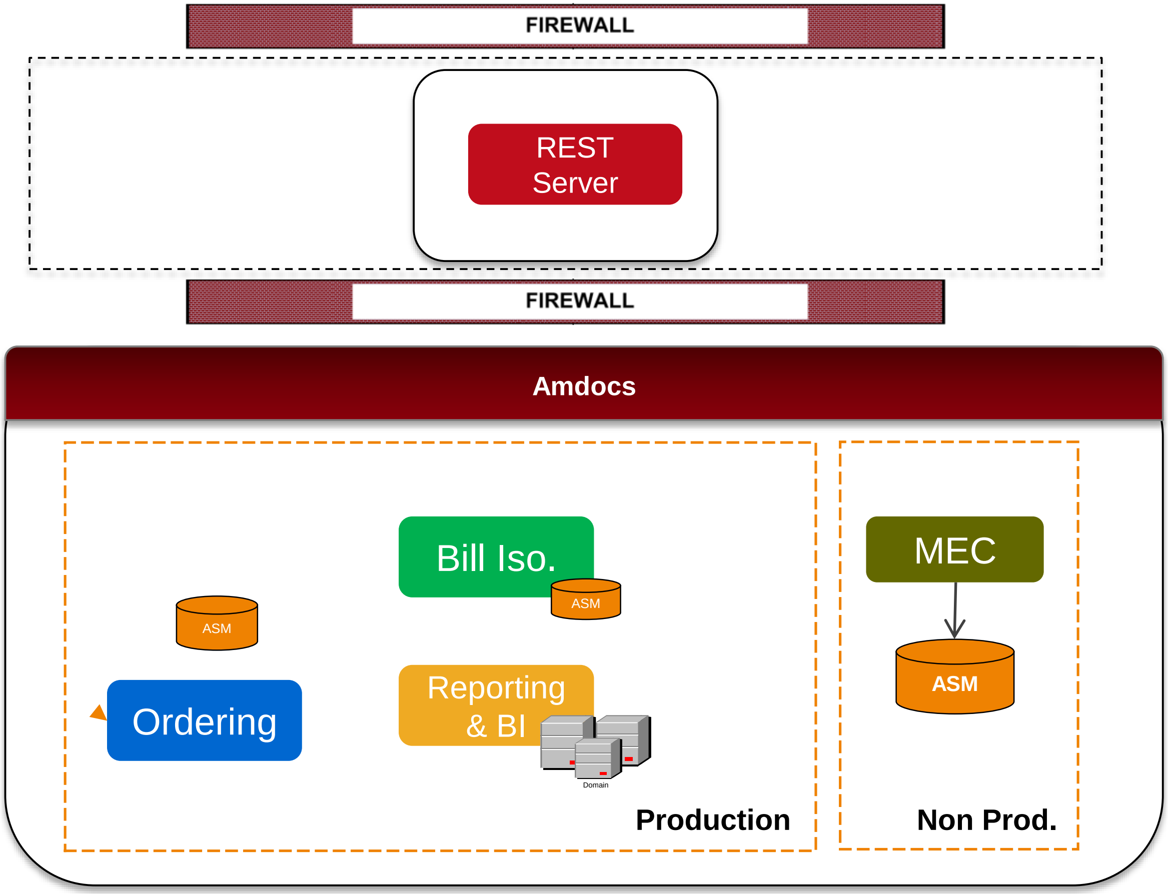
- Introduction & Solution Overview
- **Application Security**
  - Users Management
  - Authentication
  - Authorization
  - Accounting
  - Confidentiality
- Infrastructure Security
- Roles and Responsibilities
- Compliance Matrix Review
- Q&A

User Management
Users' Type

- Internal Users
  - Charter's employees – administrators, analysts, designers, technicians and so on
  - System accounts – batch/admin users, required for supporting the functionality of the system, such as batch process users, application-to-application (Gateway) calls, and so on
  - Infrastructure users – e.g. DB, OS (Under Charter's responsibility)

Users Type	Component
Back office – Charter Employees	Ordering (BE), Biller Isolation, REST, MEC, BI
Back office – System Users	Ordering (BE), Biller Isolation, REST, MEC, BI
Back office – Infrastructure Users	Charter's Infrastructure

Users Management
Users Repositories



Users Management
Administration

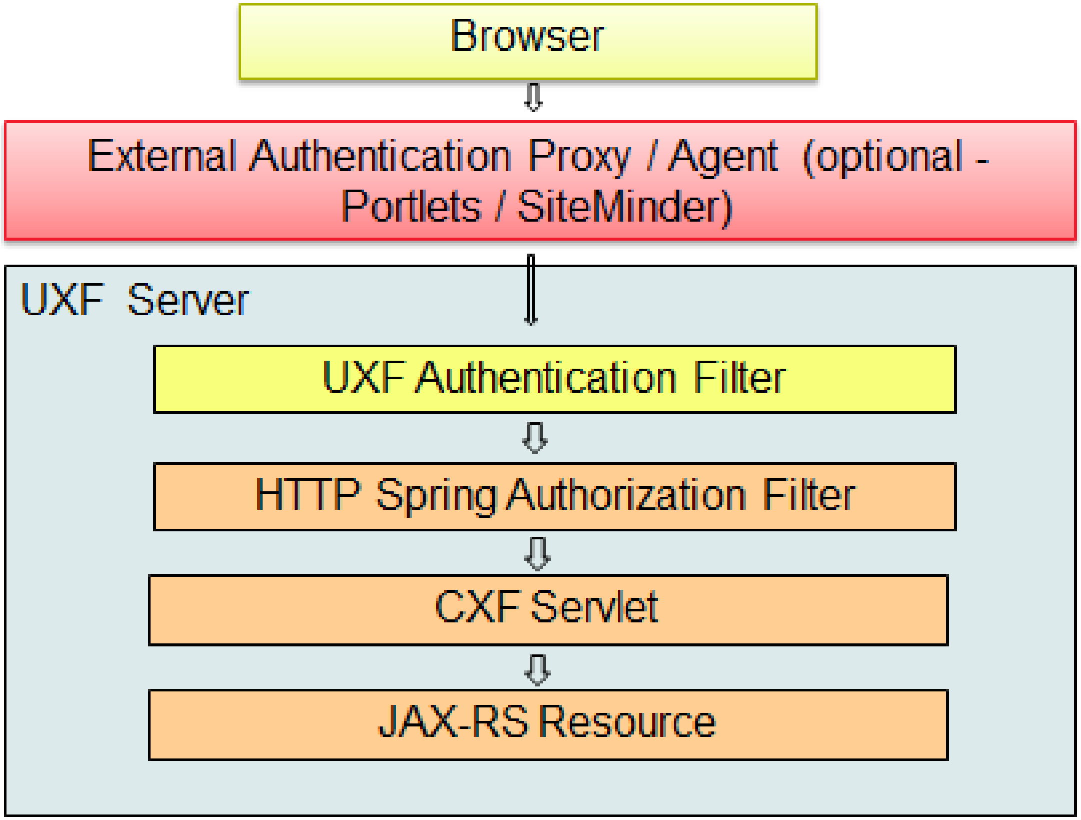
- Users records are maintained within the Amdocs system repositories

Users Type	ASM	Local	AD
Back office – Charter Employees	Ordering (BE), Biller Isolation (web-admin), MEC	Reporting & BI	
Back office – System Users	Ordering (BE), REST, MEC	Biller Isolation	
Back office – Infrastructure Users		Charter's Infrastructure	Charter's Infrastructure

- Security administration activities (e.g. create user, create role) are done through the relevant security consoles
  - ASM Administration Console (MEC, Ordering)
  - Web Admin Console (Biller Isolation)
  - Internal Admin scripts (Biller Isolation)
  - AD

Authentication

REST server

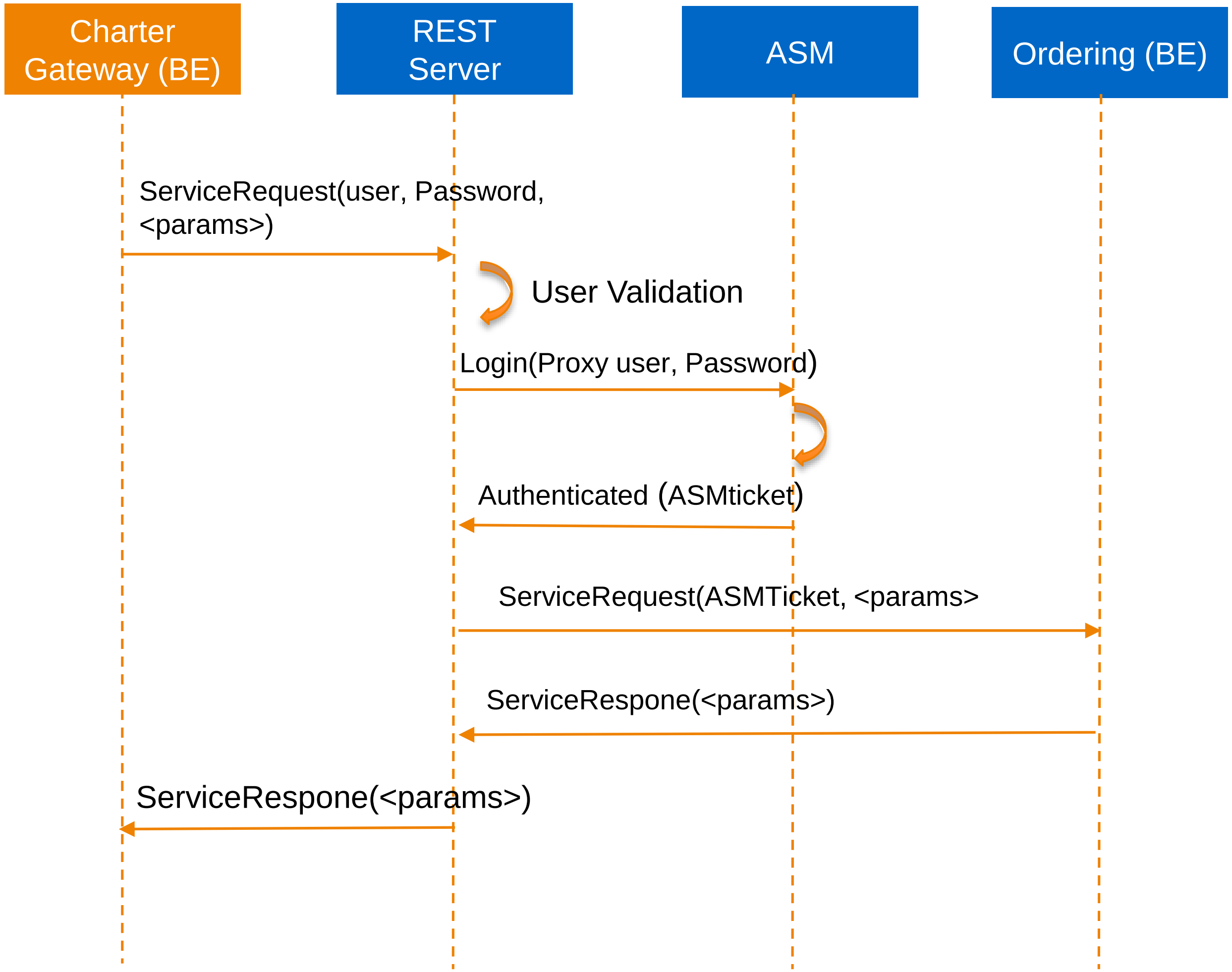

Browser
External Authentication Proxy / Agent (optional - Portlets / SiteMinder)
UXF Server
UXF Authentication Filter
HTTP Spring Authorization Filter
CXF Servlet
JAX-RS Resource

Authentication

REST server

- Charter Gateway is responsible for user authentication before consuming Amdocs REST services
- Basic authentication to the REST server
  - Charter Gateway will send proxy username and password identifying it in every request
    - Connection can be protected by SSL
  - The originator user’s information will be sent by Charter Gateway as part of the REST request (HTML header)
  - The REST server invokes a pre-defined system user for consuming internal services
  - REST services authentication to the Ordering BE is done by ASM

Authorization and Authentication
External Login


Charter Gateway (BE)
REST Server
ASM
Ordering (BE)
ServiceRequest(user, Password, <params>)
User Validation
Login(Proxy user, Password)
Authenticated (ASMticket)
ServiceRequest(ASMTicket, <params>
ServiceRespone(<params>)
ServiceRespone(<params>)

Charter

Amdocs

Authentication

MEC, Ordering, Biller Isolation

- Password based authentication (username/password)
  - Each authentication provider is responsible for its password management and login restrictions

Users Type	Charter's AD	ASM	Local
Back office – Charter Employees (Admin, Business, etc.)	Ordering (BE), Biller Isolation (web-admin), MEC, Reporting & BI		
Back office – System Users *	MEC	Ordering (BE), REST services	Biller Isolation

- ASM ticket/session is created upon successful login, which is returned to the calling application (client), and the same user ticket/session is used between all system components sharing the same ASM repository

* System users, for internal functionality (e.g. batch, jobs), are maintained in the application repository

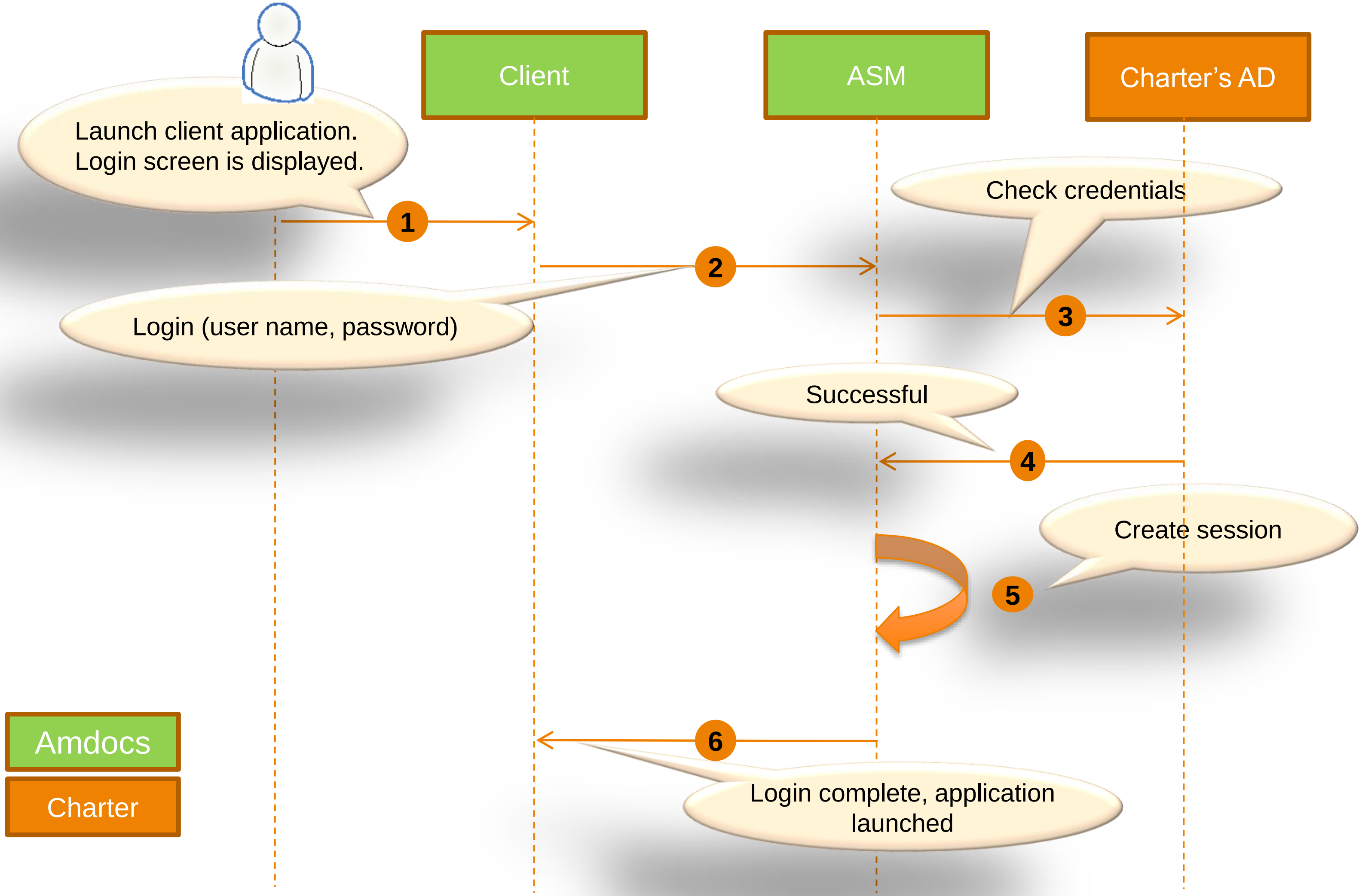
Authentication
Password Policy

Charter’s AD	Local (Biller Isolation)	ASM
Charter’s Responsibility	Passwords are created as part of the installation / modification process using manual scripts – Password policy should be enforced by the Admins creating them	• Password expiration • Minimum/maximum length • Special/numeric/capital characters • Password history • Repeating characters • Same as user name • First-time password changing enforcement mechanism • Password reset by Security Administrator • Failed login attempts

- Passwords of internal users that are authenticated against Charter’s Active Directory, will not be stored in Amdocs system.
  - Password management, including password change, will be done directly in Charter’s Active Directory and not through Amdocs system
- ASM passwords and user management will be done ASM admin

Authentication

Authentication Provider: Charter's AD (via ASM)


Client
ASM
Charter's AD
Launch client application.
Login screen is displayed.
1
2
Login (user name, password)
Check credentials
3
Successful
4
Create session
5
6
Login complete, application launched
Amdocs
Charter

Authentication
Biller Isolation - Consuming Amdocs Services

- The service consumer (Charter Gateway) should call Biller Isolation using a system user and password (user and password will be defined in Biller Isolation in advance)
- Biller Isolation will validate the login and provide the service.
- Biller Isolation is a stateless service – no session management is provided and every call is re authenticated.
- Biller Isolation supports WS security as well where the authentication can be provided by external IDP
  - Biller application can validate the authentication using the IDP public key or by consuming a service from the IDP system

Authentication

Biller Isolation - Consuming External Systems Resources

- Done using system user
  - Amdocs will store a proxy/system user and password in DB for the target systems
  - Password will be stored encrypted using AES 256 algorithm using Tomcat encryption facility.
  - User and password will be passed as part of the WS Security (SOAP)
  - All calls are assumed to be stateless
- Target system security is under Charter responsibility.
- SSL can be supported as needed.

Authentication
Files , DB and BI & reporting

- File transfer authentication will be done using the infrastructure security
- Direct access to the DB should be restructured to authorized users only
- BI & Reporting
  - Authentication will be based on Microsoft Active directory – this will be SSO based on the user authentication to his workstation.
  - Accessing external resources will be done based on the authenticated provided by the target system, credentials will be kept in the QV encrypted connection string

Authorization

- Access to Amdocs system is controlled by assigning permissions to users according to their roles
  - Each user is assigned with one or more roles according to the business needs, based on the 'Need to Know' concept
- Amdocs applications use Role Based Access Control (RBAC)
  - Role management is done through security consoles (e.g. ASM)
- RBAC implementation is business driven and is dependent on specific business requirements
  - Defining the authorization model is part of the scoping phase (BPT process)
- Biller Isolation services does not have authorization – each service is allowed to an authorized users only and the calling system should manage the authorization.

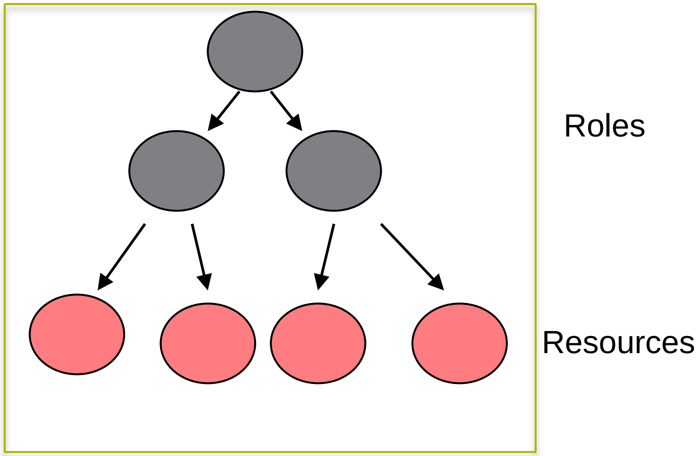
Authorization

Mapping

	Role Declaration & User/Role Linkage	Role Management	Authorization Decision Point
Ordering (BE), REST services	ASM	ASM	ASM
MEC	ASM	ASM	ASM
Biller Isolation – Admin	ASM	ASM	ASM
Biller Isolation – APIs	None	None	Biller Isolation
Reporting & BI	Internal	Internal	Internal

Authorization
ASM

- Terminology
  - Resource – protected element with a logical name (EJB API, UI element, URI, File…)
  - Business Role - represents the employee job in the organization (Manager, Analyst, …), based on the business needs
- A role can contain another role (role hierarchy)
- Each user is assigned one or more roles
- What can be controlled?
  - Resource



Authorization

REST Services

- Roles are managed in the Amdocs ASM will be Retrieved as part of the authentication to the REST server based on the user sent from the Charter Gateway
- Service consumption from the backend REST server is controlled based on user role
- Access to the rest service from the Charter Gateway can be protected using 2 way SSL.

Authorization

Reporting & BI

- All the authorization will be based on the internal definition in the application
- Permissions will be assigned to Active directory defined users
- Administrative access is using the same authorization solution

Accounting
ASM

- ASM logs are kept in DB (can be extracted - SIEM integration)
- ASM records security-related events
  - Users Management events (e.g. enable/disable of user, attach/de-attach role to user)
  - Authentication events
  - Security Administration events
- Logged Fields
  - User ID
  - Date and timestamp of transaction
  - Type of event (unique ID)
  - Success or failure indication
- Functional events are captured by the applications

Accounting
Reporting & BI, Biller Isolation

- Reporting & BI
  - Auditing is based on Microsoft windows server and the IIS capabilities
  - Every access is logged and the Active Directory account of the user is kept in the system level
- Biller Isolation
  - The web-services enables auditing with the following fields:
    - **GTXID**:global transaction id,
    - **TXID**:unique transaction id
    - **StartDate**:date of request (in milliseconds),
    - **EndDtae**:date of response (in milliseconds),
    - **ServiceName**:operationName,
    - **ModuleName:**EG/Channel name**,**
    - **SourceSystem**:USER_IP_ADDRESS,
    - **TargetSystem**:extrenal target system name,
    - **Status**:service status number (ex: 200),
    - **HandlingTime**:TOTAL_SERVER_TIME in milliseconds (endDate-startDate),
    - **ErrorCode**:Service error code,
    - **Description**:Service error description,
    - **EntityID**:orderID / CustomerID

Confidentiality

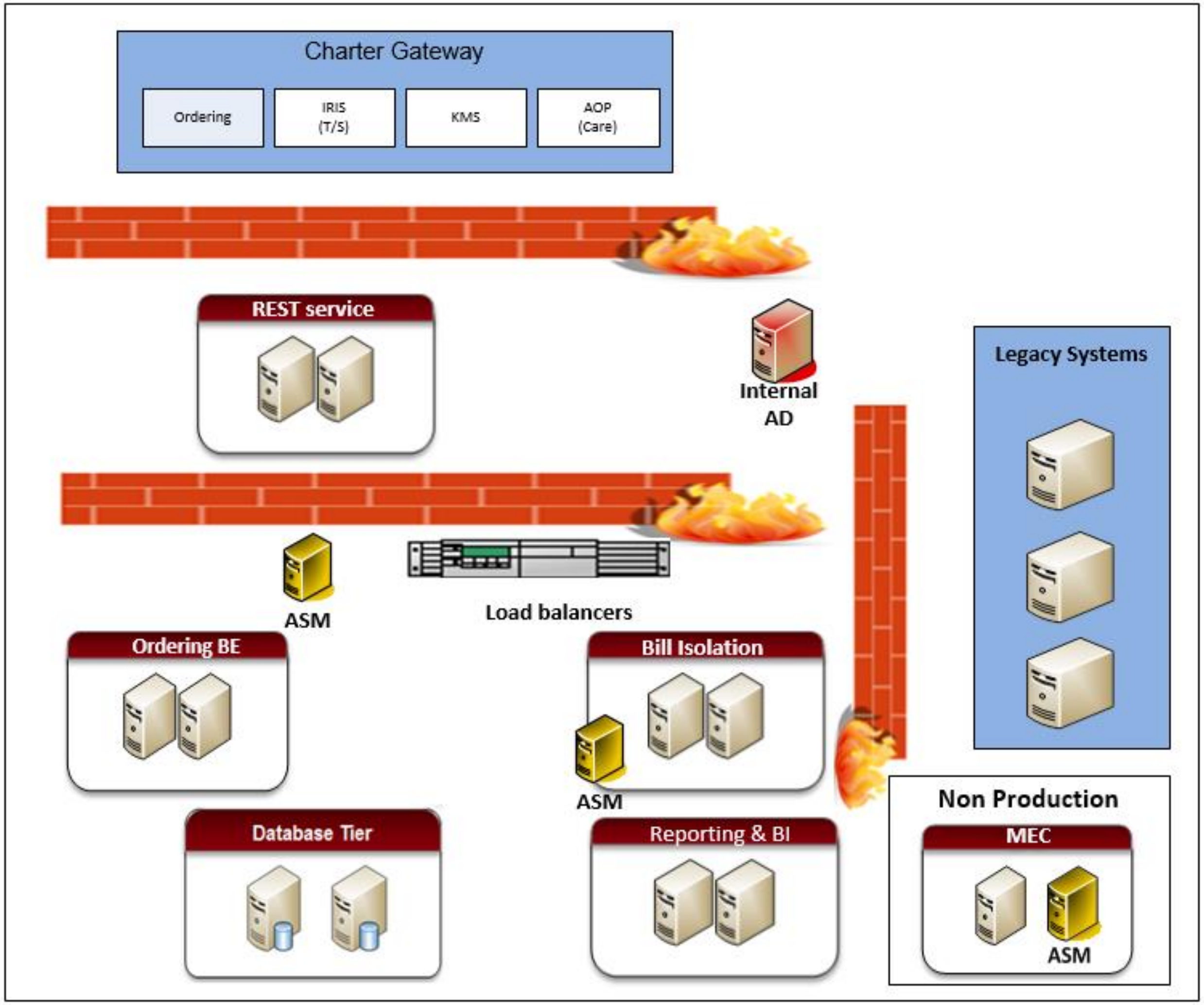
Field Type	Encrypt / Hash if stored	Field Level Logging	Mask	Scramble in QA/Dev	Acceptable for Storage	Referenced Applications
Password	Yes	Yes	Yes	Yes	Yes	All

- Users' passwords in ASM and Biller Isolation repository are hashed (SHA2)
- Passwords in properties files/DB are encrypted
- Passwords are masked / truncated in logs, display and error messages
- Sensitive information is accessible for authorized users only (roles implementation)
- Sensitive information in transit is sent over public network using HTTPS
  - Personally Identifiable Information can be encrypted on transit

Agenda

- Introduction & Solution Overview
- Application Security
- **Infrastructure Security**
  - Secured Network Design
  - Users and Privilege Management
  - System Hardening
  - Logging and Auditing
  - Access Management and Data Protection
- Roles and Responsibilities
- Compliance Matrix Review
- Q&A

Infrastructure Security



Secured Network Design

- Separated security zones using Multi tier Design
- Filtering device awareness and standard protocol use
- Separate environments for production / non-production
- Separate administration networks are supported for Out of Band (OOB) administration, system high availability, audit, and so on
- No connection to public networks
- users access will be done using Charter Gateway
- Admin access will be done from internal network only

Users and Privilege Management

- **System users**
  - Charter will manages all users on the OS level
  - Privileges are defined by Charter and enforced by them
  - Password policy is enforced in accordance to Charter policy
  - Amdocs users will be granted only the required permission to perform their work
  - Not root user is required by default – and if needed – user will ask for specific privileges add hock
- **Application/service accounts**
  - Dedicated users are used per application/service only
  - No use of root user
  - Users are granted with minimum needed privileges
  - Users will be defined and granted password as part of the installation by Charter
- **DB accounts**
  - DB accounts are managed by Charter
  - NO DBA permissions should be in use except for management tasks
  - Dedicated users are used per application/service
  - Users are granted with minimum needed privileges

System Hardening (1 of 2)

- Infrastructure hardening Can applied and must be verified against Amdocs best practices
- Every hardening process must be tested on non-production first
- Operating System
  - Boot restricted configuration
  - Support of secured protocols for remote access
  - Removal of unneeded services
  - Restricted root use
  - Enhanced password policy
  - Removal of unneeded accounts and groups
  - Enhanced access control restrictions
  - Enhanced logging configuration
  - Hardened SSH configuration

System Hardening (2 of 2)

- Database
  - Removal of unneeded / default databases
  - Cleanup of unneeded / default users and groups
  - Set up in accordance with the Least Privilege principle at operating-system level
  - Removal of unneeded extensions (HTTP server, XDB, APEX …)
  - Password policy and store hardening
  - No operating system users use
  - Limited permission for Non-DBA users
- 3rd Party Application Secure Configuration
  - Removal of unneeded content and services
  - Securing the administration interfaces
  - Reducing and reconfiguring default users
  - Refining permission sets

Logging and Auditing

- Audit Can be utilizes to allow traceability, accountability and forensics
- Infrastructure audit is based on:
  - Component's audit capabilities
  - Performance considerations
    - DB audit is not utilized by default but can be activated per specific event
  - Business needs
- Audit logs can be collected by SIEM systems
- Log rotation and retention should be configured per component and according to its storage restrictions
- Log access must be restricted and limited

Access Management and Data Protection

- Access to the system can be limited using standard FW’s
- Amdocs utilize standard protocols and allow opening only the needed ports
- FW systems should be capable of processing the traffic and correctly planned as they may cause degradation on performance
- Other security tools like DBF, IDS and other can be utilized, however each tool must be aligned with the system performance SLA and should not add latency above the system limit.
- Data at transport is protected using secured protocols
  - SSH, SFTP are utilized on the Infrastructure level
  - SSL is utilized for public access (Internet) And from Amdocs to external service
  - LDAPS is used to integrate with LDAP service

Access Management and Data Protection

- Data at rest will be protected:
  - Passwords are stored Hashed or encrypted by the relevant component
  - Backup should be encrypted by the backup application
  - Non-production Data should be scrambled or masked
  - Restricted ACL’s are implemented on file store

Agenda

- Introduction & Solution Overview
- Application Security
- Infrastructure Security
- **Roles and Responsibilities**
- Compliance Matrix Review
- Q&A

Roles and Responsibilities

Topic	Amdocs	Charter
Role Engineering	C	R
RBA Implementation	C	R
Users’ Creation	-	R
Security Technical Parameters	C	R

R = Responsible

C = Contributor

Agenda

- Introduction & Solution Overview
- Application Security
- Infrastructure Security
- Roles and Responsibilities
- **Compliance Matrix Review**
- Q&A

Compliance Matrix Review

Microsoft Excel Worksheet

Agenda

- Introduction & Solution Overview
- Application Security
- Infrastructure Security
- Roles and Responsibilities
- Compliance Matrix Review
- **Q&A**

Thank You