Identity and “Access” Management

PRESENTATION TO CORKSEC MEETUP #61
BY ROBERT LAMBERT

Identity and “Access” Management

WHY “ACCESS” MANAGEMENT IN QUOTES?

THERE ARE TWO PARTS TO THIS

- IDENTITY MANAGEMENT = WHO ARE YOU?
- ACCESS MANAGEMENT = YOUR ACESS RIGHTS?

THE FIRST IS COVERED BY IDM (Identity Management)

INCLUSION OF THE ACCESS IS IAM (IDM + Access)

CONTEXT IN THE AREA OF SECURITY?

ANALOGY OF A CASTLE AND ITS DEFENDERS

- CASTLE WALLS & TOWERS (Software, Networks Firewalls etc)
- TROOPS & INHABITANTS WITHIN THE DEFENCES (Users access to data, what, how much, what are they allowed to do with data)

SENTRY: “WHO GOES THERE?” (Who is allowed access…)

DON’T WANT INVADERS TAKING OVER THE CASTLE USING THE FACT THAT THOSE WITHIN HAVE UNIVERSAL ACCESS TO DATA

IN THE CONTEXT OF IT GOVERNANCE

HAVING WELL DEFINED SECURITY AND DATA ACCESS POLICIES ARE KEY PARTS OF THE FOLLOWING:

- GDPR
- SOX
- HIPPA
- BASEL II

THIS IMPLIES WELL DEFINED AND CONTROLLED DATA ACCESS MANAGEMENT SYSTEMS MUST BE IN PLACE

KEY CONCEPTS

- **USERS** – THESE CAN BE HUMAN OR MACHINE, BUT WE'LL FOCUS MAINLY ON HUMAN
- **ROLES** – THESE CAN BE JOB ROLES, FROM WHICH IT IS DETERMINED WHAT ACCESS TO DIFFERENT SYSTMS AND WHAT PRIVELEGES EACH USER IS ALLOWED

KEY CONCEPTS

IDENTITY & ACCESS MANAGEMENT	A system of procedures, policies and technologies to manage the lifecycle & entitlements of electronic credentials
DIRECTORY SERVICES	Repositories for storing & managing accounts, identity information, & security credentials
ACCESS MANAGEMENT	Process of authenticating credentials & controlling access to networked resources based on trust & identity
IDENTITY LIFECYCLE MANAGEMENT	Processes used to create & delete accounts, manage account & entitlement changes, and track policy compliance

CAN WE IMPLEMENT USING AD?

- YES AND THAT'S WHERE MANY ACCESS MANAGEMET SYSTEMS START & END
- THIS WORKS WELL FOR SMALL AND STABLE IT INFRASTRUCTURES
- IT DOES REQUIRE A VERY WELL DEFINED SET-UP OF AD, WHICH MATCHES THE ORGANISATION STAFF AND THEIR ROLES
- IT REQUIRES THE ABILITY TO ENSURE SYNCHRONISATION OF DIFFERENT SYSTEMS WITH USERS EASILY PROVISIONED, CHANGED OR REMOVED

WHY IS FORMAL IAM IMPLEMENTED?

BECAUSE…

- NEED FOR FORMAL SOLUTION AS USER NUMBERS GROW
- USER/STAFF TURNOVER INCREASES
- IT DEPARTMENTS CANNOT COPE WITH ACCOUNT PROVISIONING
- IT DEPARTMENTS ALSO STRUGGLE WITH SUPPORT (SELF SERVICE)
- TYPICALLY AD SOLUTIONS BREAK DOWN AS WELL (SECURITY)
- ALSO GETS VERY COSTLY TO MAINTAIN EXISTING SET-UP

IAM IMPLEMENTATIONS?

- TYPICALLY START WITH ACTIVE DIRECTORY WHEN YOU'RE SMALL
- GROW (WITH USER TURNOVER) & MORE APPLICATIONS ADDED
- THEN AD & APPLICATION USER ACCOUNTS BECOME PAINFUL TO MANAGE
- NOW NEED TOOLS TO MANAGE USERS & ACCOUNTS…
- INTRODUCE IAM to MANAGE KEY APPLICATIONS INITIALLY FOR USERS WITH BASIC RESTRICTED ROLES
- MAY THEN WORRY ABOUT ROLE BASED ACCESS
- THEN INTEGRATE MORE APPLICATIONS FOR USERS

WHAT ARE THE KEY SOLUTIONS?

- FIM/MIM (Microsoft)
- OIM (Oracle)
- NETIQ (Formerly Novell)
- SAP (has own solution)
- LINUX BASED
- OTHERS… (many of them)

METHODOLOGY

- IAM IMPLEMENTATION IS GOVERNANCE & BUSINESS PROCESS INTENSIVE
- SURE YOU CAN DO AN OUT-OF-THE-BOX AS AN EASY FIRST STEP
- THEN YOU HAVE TO DETERMINE YOUR COVERAGE
- THEN UNDERGO CYCLES OF INTEGRATIONS?

Business Analysis Requirements

- Roles and access must be define? How?
- USE CASES
- By Department
- By User Role
- Data Sensitivity / Security (least access granted)
- Compliance e.g GDPR
- Application internal defined roles per application (admin/user or more?)

Application Defined Roles…

- THIS IS OFTEN OVERLOOKED
- SOME ARE VERY SOPHISTICATED & FLEXIBLE
- OTHER ARE OLD & INFLEXIBLE (Admin.Write.Read only)
- Are there external or intergation interfaces?
- Is SSO (Single Sign-on) possible?

ITS NOT JUST INTERNAL USERS

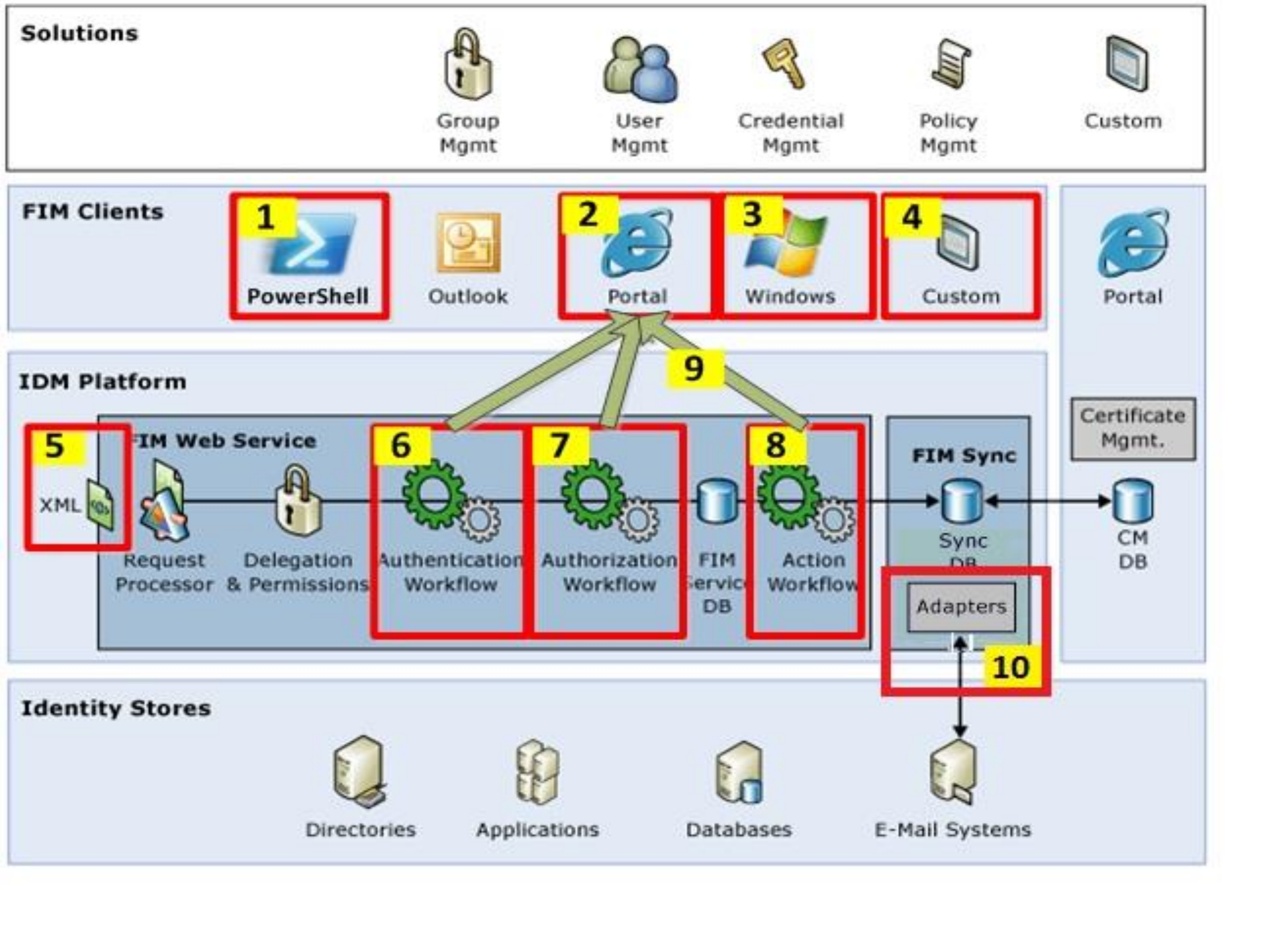
- Customer IAM
- Federated Access
- Data Sharing & External Co-operation

THIS DRIVES FURTHER TECH REQUIREMENTS INCLUDING…

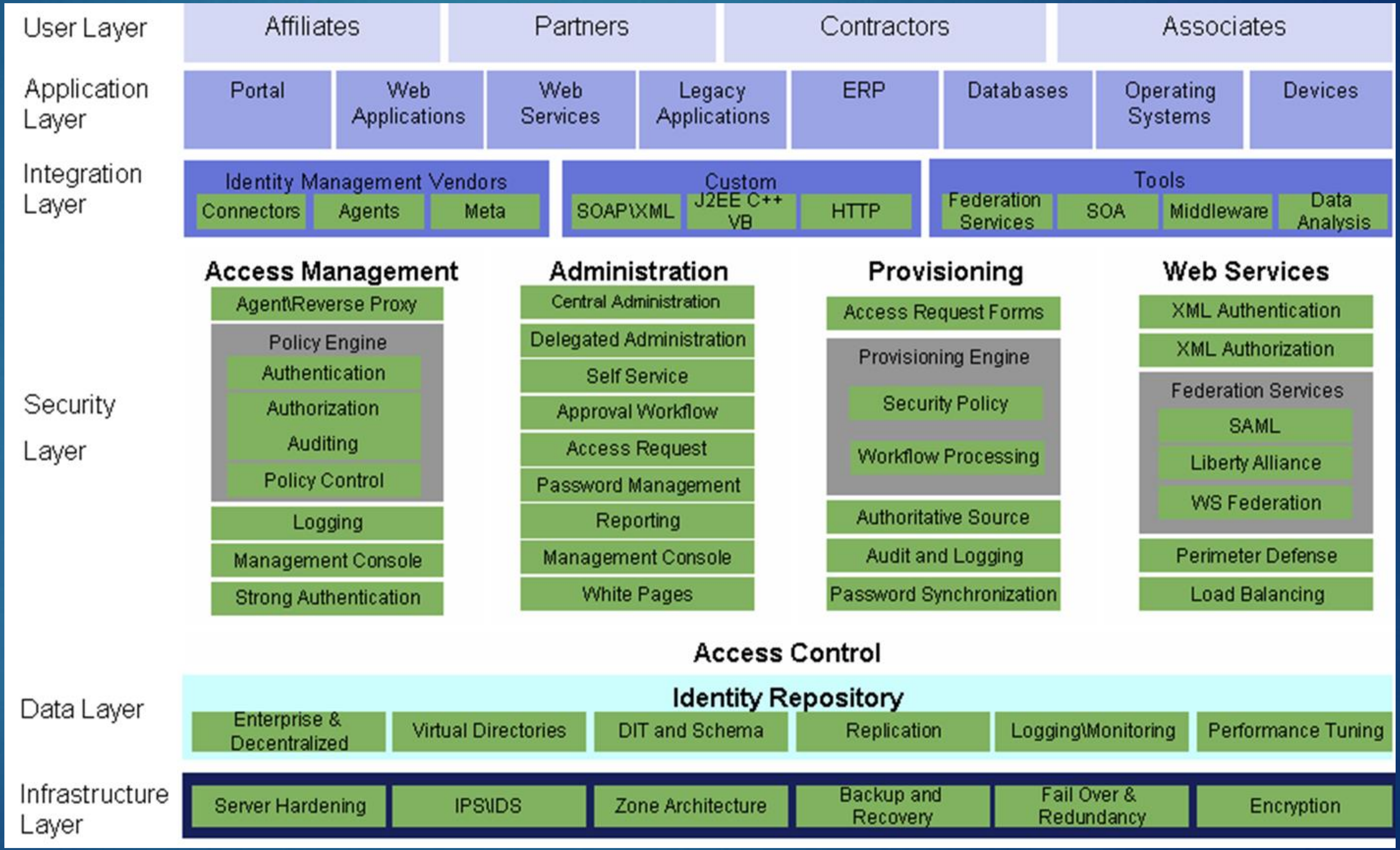
- Additional IAM systems, typically customer online accounts
- Other security provisions including policy, firewalls etc…

EXAMPLE ARCHITECTURE (1)

FIM/MIM (Microsoft)



MORE DETAILED VIEW



User Layer
- Affiliates
- Partners
- Contractors
- Associates

Application Layer
- Portal
- Web Applications
- Web Services
- Legacy Applications
- ERP
- Databases
- Operating Systems
- Devices

Integration Layer
- Identity Management Vendors: Connectors, Agents, Meta
- Custom: SOAP\XML, J2EE C++ VB, HTTP
- Tools: Federation Services, SOA, Middleware, Data Analysis

Security Layer

Access Management
- Agent\Reverse Proxy
- Policy Engine
  - Authentication
  - Authorization
  - Auditing
  - Policy Control
- Logging
- Management Console
- Strong Authentication

Administration
- Central Administration
- Delegated Administration
- Self Service
- Approval Workflow
- Access Request
- Password Management
- Reporting
- Management Console
- White Pages

Provisioning
- Access Request Forms
- Provisioning Engine
  - Security Policy
  - Workflow Processing
- Authoritative Source
- Audit and Logging
- Password Synchronization

Web Services
- XML Authentication
- XML Authorization
- Federation Services
  - SAML
  - Liberty Alliance
  - WS Federation
- Perimeter Defense
- Load Balancing

Access Control

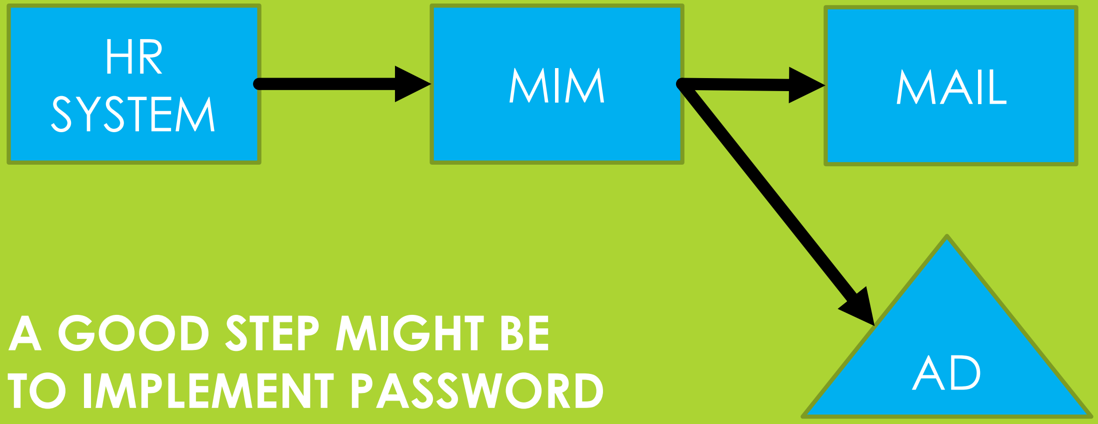
Data Layer

Identity Repository
- Enterprise & Decentralized
- Virtual Directories
- DIT and Schema
- Replication
- Logging\Monitoring
- Performance Tuning

Infrastructure Layer
- Server Hardening
- IPS\IDS
- Zone Architecture
- Backup and Recovery
- Fail Over & Redundancy
- Encryption

STEP 1 MIM - Basics

- OUT-OF-THE-BOX, THIS REPLACES EXISTING AD IMPLEMENTATION



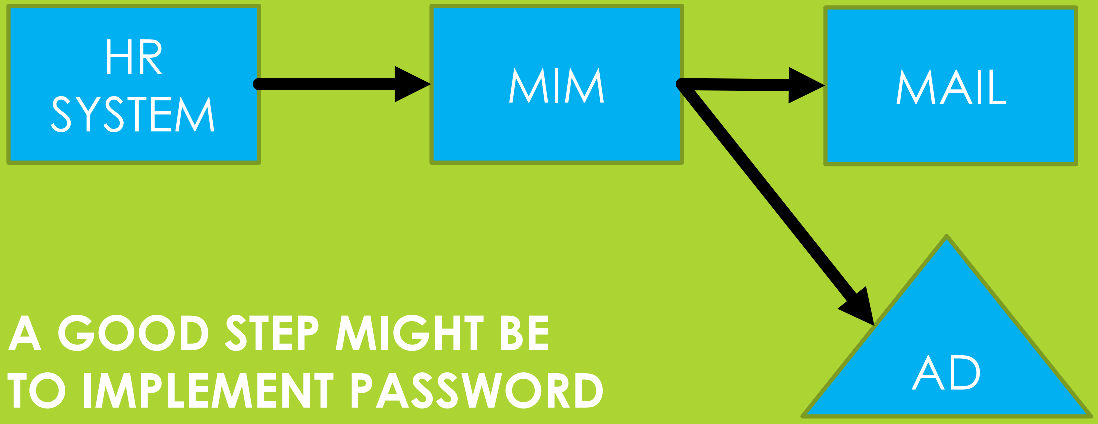
A GOOD STEP MIGHT BE TO IMPLEMENT PASSWORD SELF-SERVICE AS WELL

Step 1 MIM – Early Wins

- Single Sign-on
- Password Self Service
- New User Provisioning
- Clearing out old users
- Printer Access

STEP 2 – User Roles Further Work

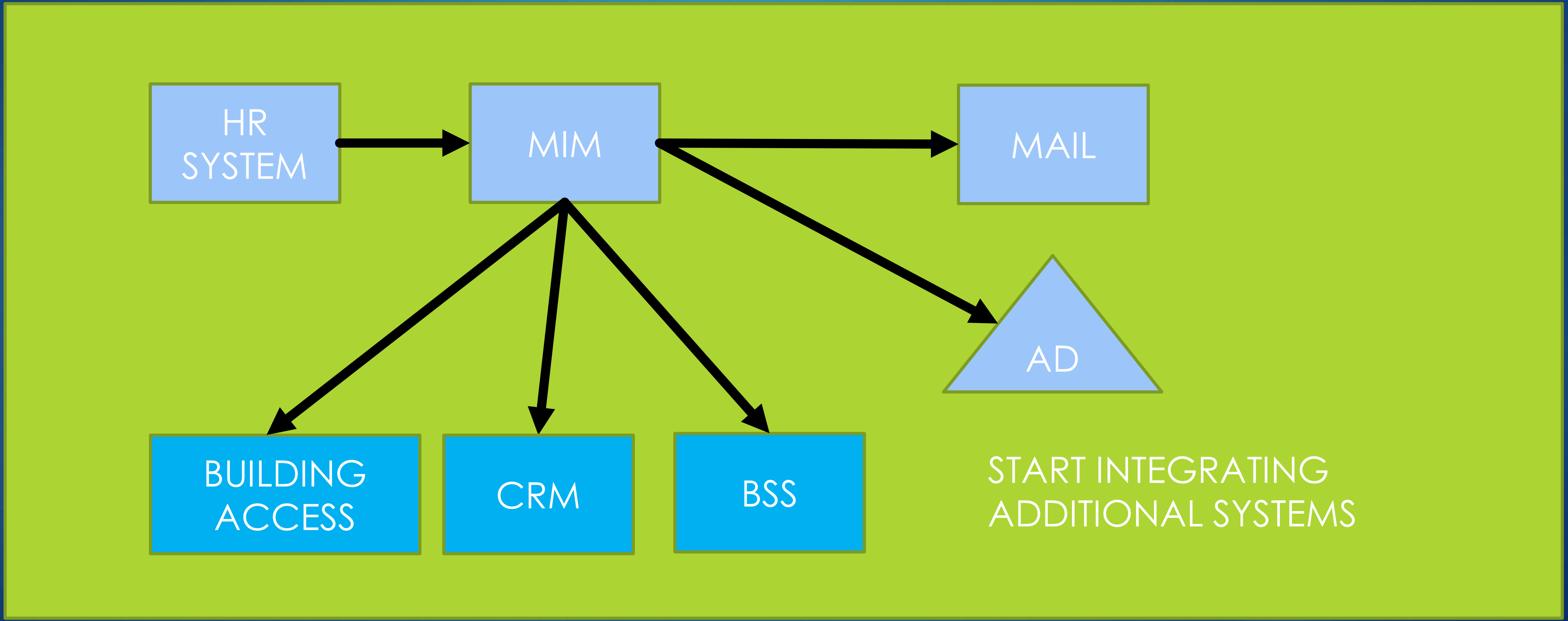
- USER ROLES COULD BE FURTHER DEFINED ESPECIALLY IF NEW SYSTEMS ARE TO BE ADDED. USE CASES FOR ROLE AND SYSTEM ACCESS REQUIRED



A GOOD STEP MIGHT BE TO IMPLEMENT PASSWORD SELF-SERVICE AS WELL

STEP 3 – Integrate Additional Systems

- START ADDING OTHER BUSINESS SYSTEMS



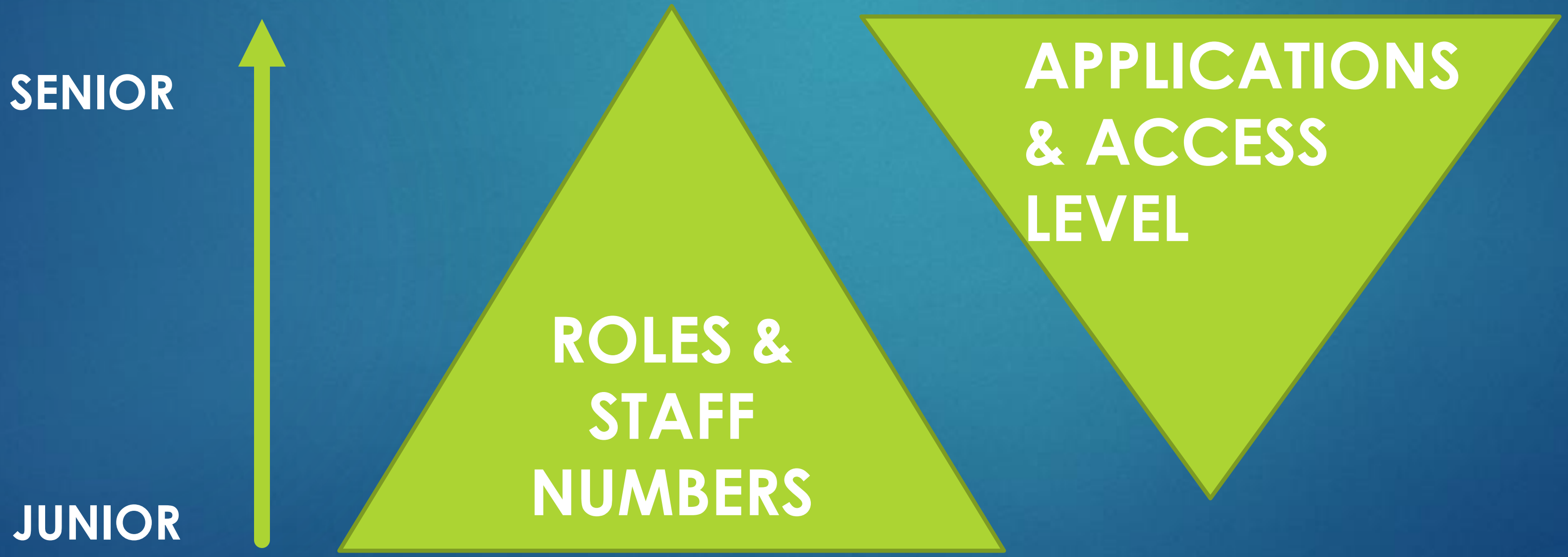
START INTEGRATING ADDITIONAL SYSTEMS

INTEGRATION CHALLENGES

- ADDING IN OTHER SYSTEMS… Data compatibility?
- AD WORKS AGAINST YOU… Need to separate AD groups?
- PROPRIETRY INTERFACES… can they be hooked up?
- STRANGE PROTOCOLS…

SENIOR VS JUNIOR STAFF (ACCESS REQUIRED?)

- Inverting the triangle…
- Picture two triangles – one inverted staff roles vs systems needed
- For every system required admin support also needed



SENIOR

JUNIOR

ROLES & STAFF NUMBERS

APPLICATIONS & ACCESS LEVEL

HOW FAR DO YOU TAKE IAM?

- In practice not feasible to IAM everything, some applications gets left at AD? Especially those used by tech support or systems with very sensitive information only to be accessed by a very restricted user group.
- In practice IAM a journey with steps…

OTHER CONSIDERATIONS

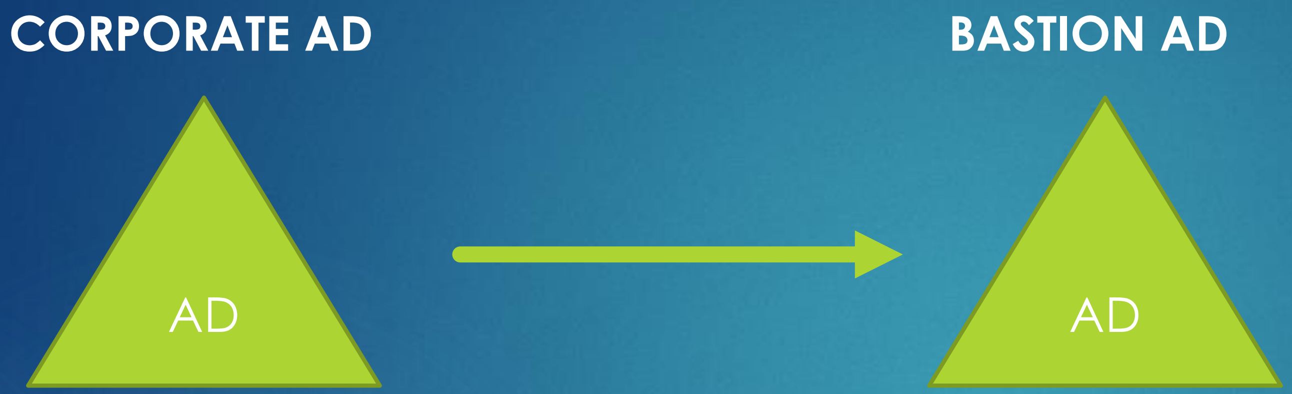
- END USER READINESS
- CLOUD ACCESS
- MOBILE DEVICES
- SINGLE SIGN ON FOR ADDITIONAL DEVICES
- PRIVELGED ACCESS MANAGEMENT

ADMIN ACCESS?

CHALLENGES

- Don’t want hackers to have “keys to the kingdom”…
- Privileged Access Management (PAM)
- Background is that admin accounts have been hacked by Spearphishing attacks, which allowed lateral movement within organisation gaining further access.
- So you need a just-in-time and just enough admin to carry out tasks and then remove this access.

PRIVILEGED ACCESS MANAGEMENT

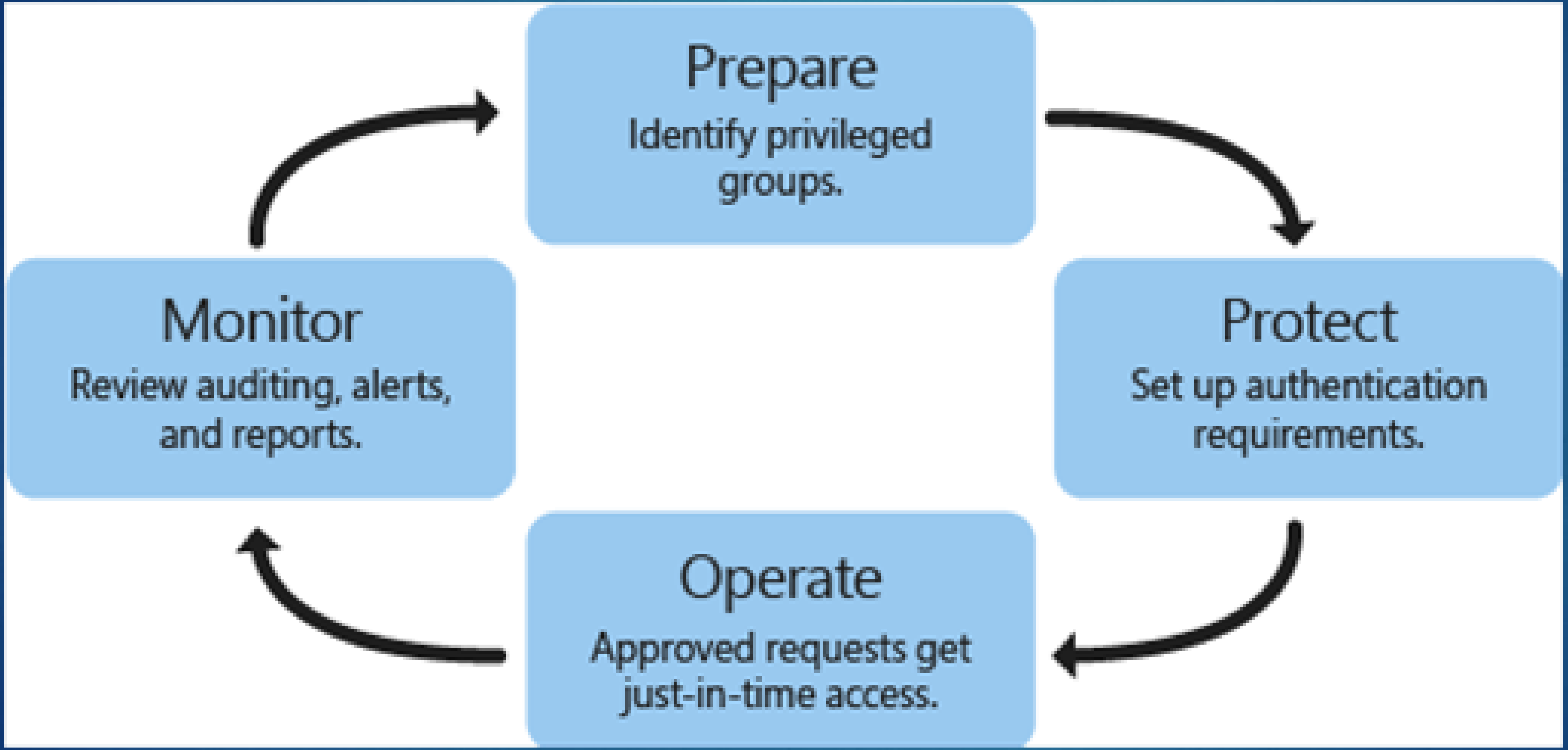


A USER IS GIVEN TEMPORARY PRIVILIGED ACCESS TO A BASTION AD WHERE THE CRITICAL WORK IS EXECUTED
THIS IS AUTHORISED BY ANOTHER HUMAN USER
THEY ACCESS VIA A JUMP SERVER
THE ACCESS WILL BE TIME OUT

https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

© Microsoft

PRIVILEGED ACCESS MANAGEMENT



Prepare
Identify privileged groups.

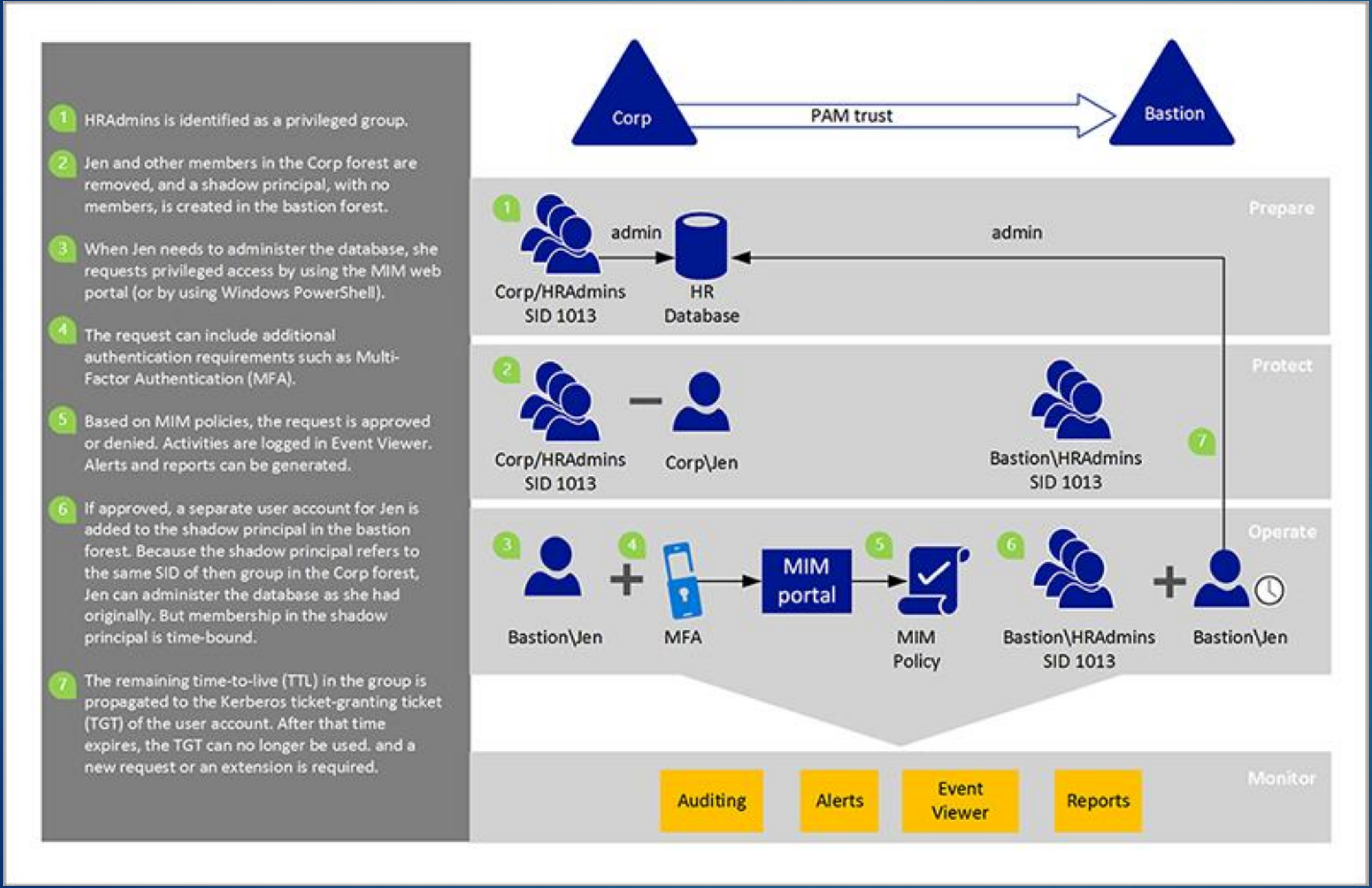
Protect
Set up authentication requirements.

Operate
Approved requests get just-in-time access.

Monitor
Review auditing, alerts, and reports.

© Microsoft

PRIVILEGED ACCESS MANAGEMENT



1. HRAdmins is identified as a privileged group.
2. Jen and other members in the Corp forest are removed, and a shadow principal, with no members, is created in the bastion forest.
3. When Jen needs to administer the database, she requests privileged access by using the MIM web portal (or by using Windows PowerShell).
4. The request can include additional authentication requirements such as Multi-Factor Authentication (MFA).
5. Based on MIM policies, the request is approved or denied. Activities are logged in Event Viewer. Alerts and reports can be generated.
6. If approved, a separate user account for Jen is added to the shadow principal in the bastion forest. Because the shadow principal refers to the same SID of then group in the Corp forest, Jen can administer the database as she had originally. But membership in the shadow principal is time-bound.
7. The remaining time-to-live (TTL) in the group is propagated to the Kerberos ticket-granting ticket (TGT) of the user account. After that time expires, the TGT can no longer be used. and a new request or an extension is required.

© Microsoft

THANK YOU

- ROBERT LAMBERT
- robbielambert@gmail.com
- 087-2686060
- Independent contractor, who has worked with the design, deployment and security of large scale systems and security in the IT and Telecoms sectors.