DIPLOMA IN CLOUD SECURITY

Project Assignment 5:

Identity and Access Management

By

Juan José Para Catalá

15nd December 2018

Table of Contents:

	Page(s)
Background	3
Create an Identity and Access Management strategy for the new system IAM Organizational Overview Strategy and Planning Team Product Team Technical Team Architecture Team	4
Outline how you would manage access Set up Cloud Identity Permissions for project CARS	5 - 6
Centralized Access Control	7
Enterprise-level: functional permissions	7 - 8
Conclusion	8

Background

The Department of Transportation is composed of a number of different agencies, including the Office of the Secretary of Transportation (OST) and the National Highway Traffic and Safety Administration (NHTSA), but also encompasses aviation, rail, maritime and even pipeline administrations. On June 24, 2009, President Obama signed the Consumer Assistance to Recycle and Save (CARS) Act, which directed the Secretary of Transportation (acting through NHTSA) to establish and administer what would come to be popularly known as the "cash for clunkers" program. The Car Allowance Rebate System, was a $3 billion U.S. federal scrappage program intended to provide economic incentives to U.S. residents to purchase a new, more fuel-efficient vehicle when trading in a less fuel-efficient vehicle. The program was promoted as providing stimulus to the economy by boosting auto sales, while putting safer, cleaner and more fuel-efficient vehicles on the roadways. NHTSA was called on to lead the CARS program at the implementation level. Given the sheer size and scope – and just a 30 day timeline – everyone who could be spared within the DOT was pulled onto the project. That meant leveraging as many existing resources and services as possible, as well as working closely with DOT partners, systems and networks to make this mandate happen. Cloud computing was one obvious way to realize the kind of scale and speed that was required. However, at the time, cloud computing seemed to offer more problems than solutions, presenting security challenges that appeared to be incompatible with the government's certification and accreditation process. There was also the issue of the extensive eligibility requirements for consumers to trade in their cars.

They were the following: ▪ Vehicle must be less than 25 years old on the trade-in date. ▪ Only the purchase or 5-year minimum lease of new vehicles qualify. ▪ Generally, trade-in vehicles must get a weighted combined average rating of 18 or fewer miles per gallon (some very large pickup trucks and cargo vans have different requirements). ▪ Trade-in vehicles must be registered and insured continuously for the full year preceding the trade-in. ▪ Trade-in vehicles must be in drivable condition. ▪ The program ran from July 1, 2009 until August 24, 2009. ▪ The program requires the scrapping of the eligible trade-in vehicle and that the dealer disclose to the customer an estimate of the scrap value of the trade-in. The scrap value, however minimal, will be in addition to the rebate, and not in place of the rebate. ▪ The new car bought under the plan must have a suggested retail price of no more than $45,000, and for passenger automobiles, the new vehicle must have a combined fuel economy value of at least 22 mpg. The CARS program will be administrated through a central system that will be accessible by car dealers involved in the program and centrally managed by the NHTSA. The system will track the incoming and outgoing vehicles, as well as consumer information and eligibility requirements. The program will need to be central so as to track vehicles and consumers. The 'clunkers', that the car dealer received were not allowed be resold. To ensure that vehicles traded-in under were not resold by dealers, the program outlines a procedure for destructively disabling the engine. You have been contracted by the company as IT security manager to assess the security concerns surrounding the CARS program being hosted in the cloud. Your findings will form a security report.

1. Create an Identity and Access Management strategy for the new system. Users, administrators etc. should all have different levels of access. Describe the different levels of proposed access.

IAM Organizational Overview

Under the direction of the IAM Program Director, the IAM program is organized into four distinct teams: Strategy and Planning, Product, Technical, and Architecture.

Strategy and Planning Team (Juan Para, employee 1, employee 2, employee 3)

The IAM Strategy and Planning Team is responsible for providing communication, strategic planning, and Outreach across the Country (cars dealers), NHTSA, OST and the IAM program itself.
Staff will be added to assist in the development of the focus areas listed below:

- Program Plan Creation
- Community Planning and Outreach
- Cloud Infrastructure Planning
- Communications
- IAM Human Resources
- IAM Finance

Product Team (Juan Para, employee 1, employee 4, employee 5)

The IAM Product Team provides functional and product support, including business process evaluation, service definition, and the development of IAM as a series of supportable products. Staff will be added to assist in the development of the focus areas listed below:

- Business Analysis
- Service Definition
- Product Management
- Solution Support Services
- Quality Assurance

Technical Team (Juan Para, employee 1, employee 6, employee 7)

The IAM Technical Team implements, tests, and releases the IAM solution set. Staff will be added to assist in the development of the focus areas listed below:

- Project Planning
- Identity Management
- Access Management
- Identity Repositories
- Practice Management
- Systems Integration

Architecture Team (Juan Para, employee 8, employee 9, employee 10)

The IAM Architecture Team provides subject-matter expertise, best practices and patterns for implementation, technical problem resolution approaches, and strategic direction recommendations. Responsibilities include:

- IAM Policy Creation
- IAM Solution Architecture and Design
- Government IAM Standards

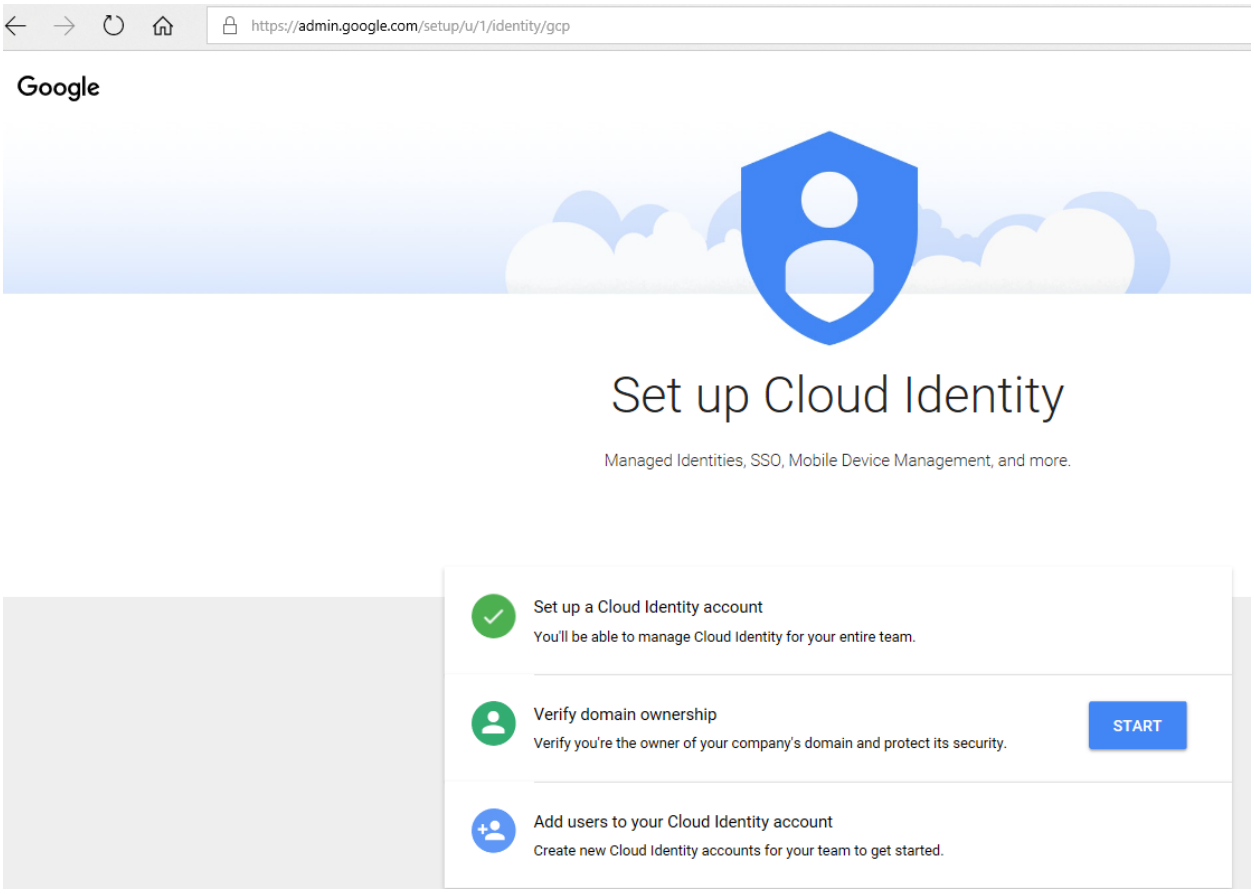
https://www.ibm.com/security/services/identity-access-management/strategy-and-assessment-services

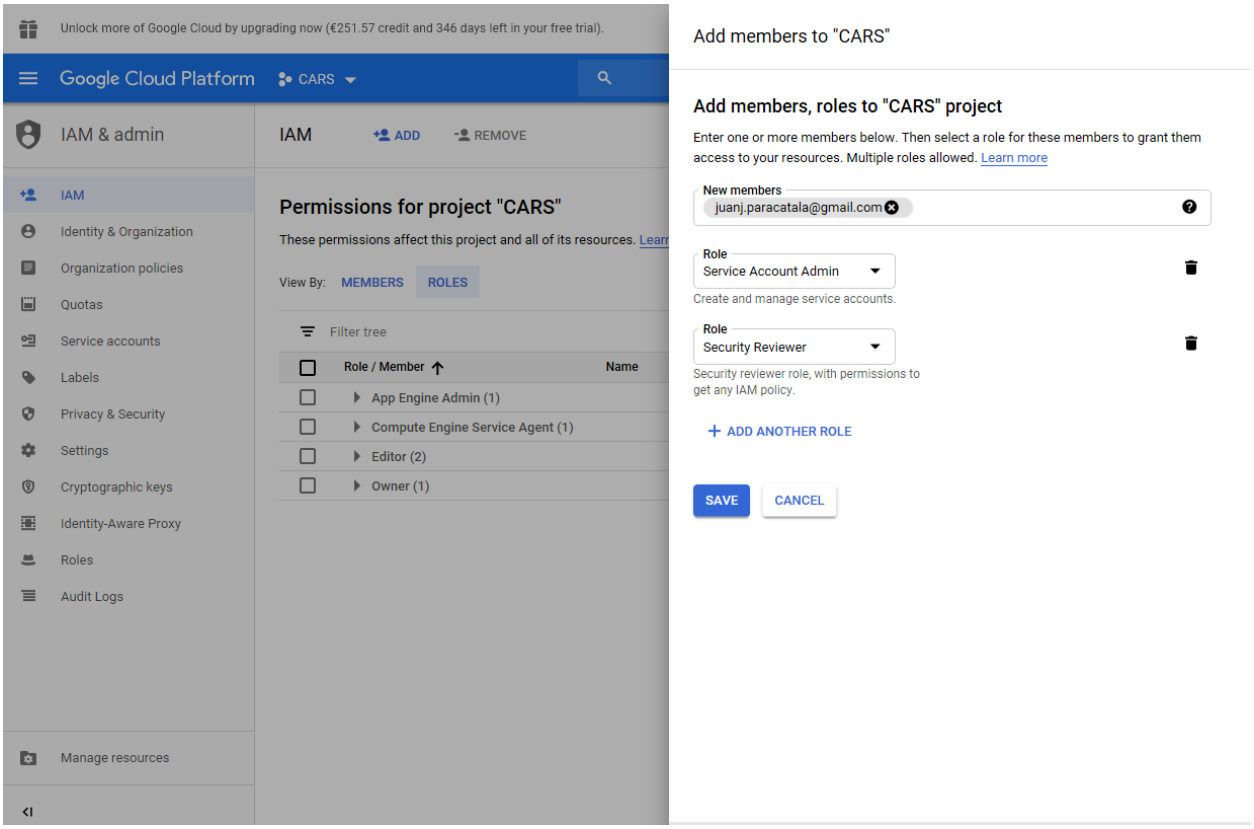
2. Outline how you would manage access (e.g. digital identities).

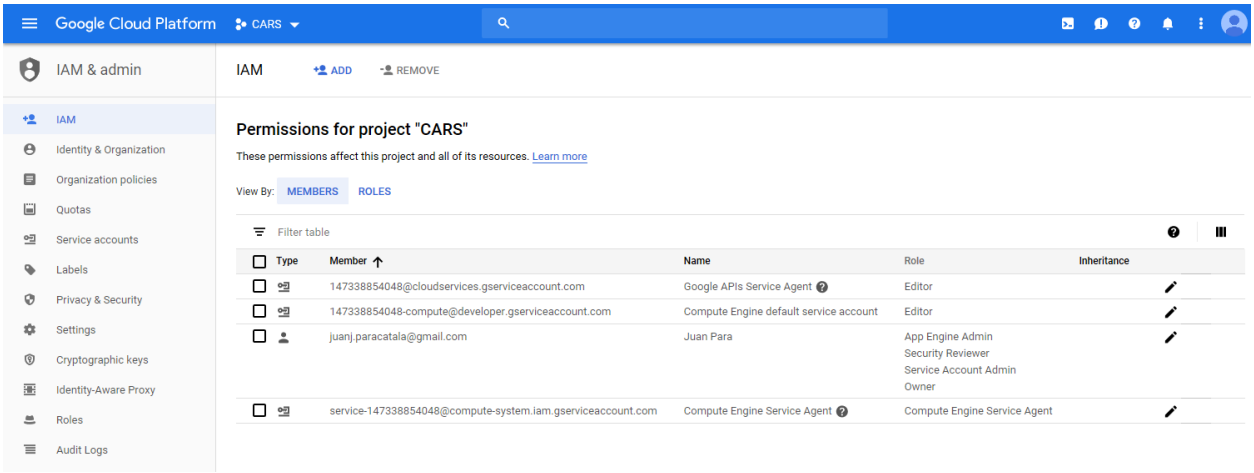
Digital Identity Management its refers for **example**, an email application defines an identity via a login, password.

Below we are going to see in a very basic way how could we grant access or assign roles within the project CARS to these fictional employees 1 to 10.

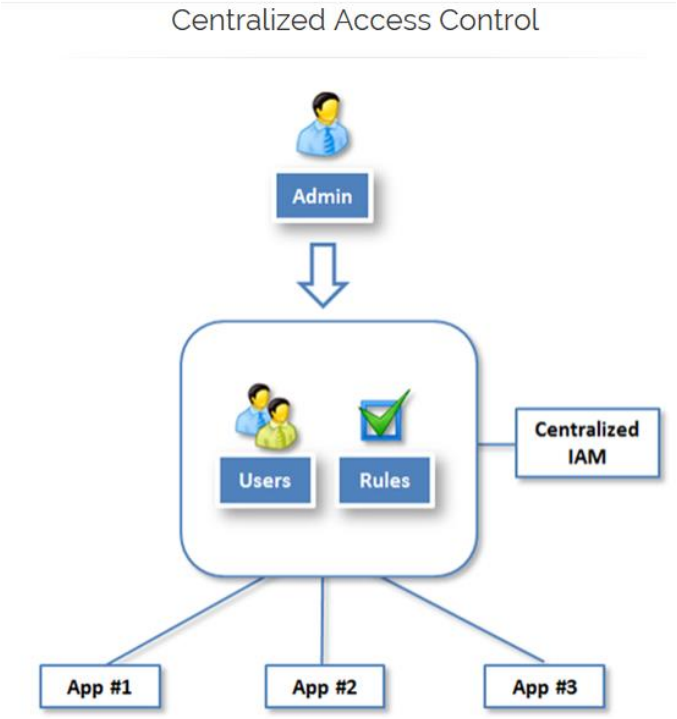
However, because per each employee Google requires or demand a real email address, here I will be using my own email address.







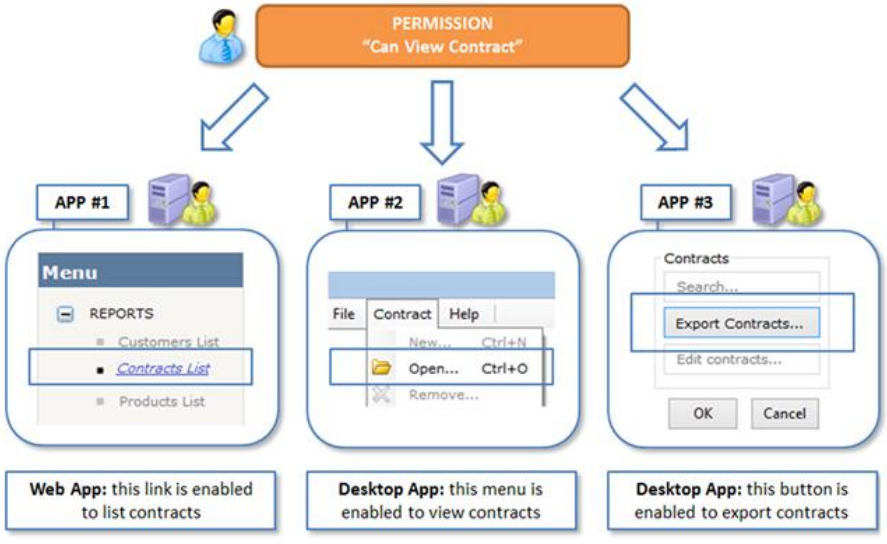
To grant access we have an identity, roles and resources, these resources comes from App engine.



Enterprise-level: functional permissions

The permission is associated to an operation and a job entity (create an invoice, consult a contract…). Functional permissions can be common to multiple applications. They are defined by those specialized in the job and/or access control. Each development team then breaks down the functional permissions into technical actions. For example, the permission “CanViewContract” could act on forms, menus, buttons, etc. allowing to consult contracts in multiple applications.

Functional Permissions



Enterprise-level permission

Granting/revoking 1 functional permission instantly secures several applications:
Security administrators declare a single - business oriented - permission
Each development team transposes this permission into specific changes in their applications
Security administrators do not need to know the applications when they grant functional permissions

https://www.visual-guard.com/EN/net-powerbuilder-application-security-authentication-permission-access-control-rbac-articles/dotnet-security-article-ressources/iam-best-practices.html#permissionsvsrbac

Conclusion

Identity and Access Management (IAM) solutions generally focus on identity management (user accounts) and coarse-grained permissions. They see applications as monolithic resources to which a user can, or not, access. This type of “all or nothing” control only protects the exterior of the application. However, users do not have all the same access rights within a company. We need to go further and define what users can do inside applications with fine-grained permissions. This need is often covered by writing custom code in each application.
The Google Cloud Platform IAM service is simple and its outstanding features include GCP Project, Policy Inheritance, and Role Creation according to job functions. However, in comparison with others Cloud providers’ IAM, GCP still requires some improvements such as custom policies and user group creation. Nonetheless, GCP IAM serve the basic purpose of controlling and managing cloud resources efficiently. IAM is a must-use service for better user and resource management, as well as enhanced security.

https://www.stratoscale.com/blog/compute/comparing-google-iam-aws-iam/