# IDPro Body of Knowledge - Demo

Principal Editor: TBD

January 31, 2019

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Authentication

This section is about recognizing the person or system accessing a computer resource, such as a file or a transaction.

Below is a sample table

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed consectetur, neque id viverra vulputate, nisi dui vestibulum quam, vel rhoncus odio est eget est. Integer vel ex vel velit ornare tristique. Sed convallis arcu tellus, eget tincidunt eros tempor vitae. Sed ultrices tellus id viverra porttitor. Aliquam eros sapien, consectetur vel imperdiet vel, fermentum in erat. In bibendum convallis lobortis. Maecenas vitae tempus elit. Duis vitae quam luctus nibh placerat bibendum. Sed et sapien velit. Vivamus erat purus, eleifend sed sapien ac, luctus rutrum eros. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aenean nec quam at nisl egestas suscipit. Nunc tincidunt lacinia purus, sed volutpat eros consequat non. Donec in euismod elit.

Nulla a commodo nibh. Vivamus in quam tempus, commodo ipsum sit amet, tempus massa. Sed non libero nisi. Integer auctor, nisl nec imperdiet cursus, enim est hendrerit

Table 1.1: Components of Authentication

| Component | Description |
|---|---|
| Identifier | How the system knows which user or system is in question |
| Credentials | Some set of things that “proves” that the identifier is being used by the “right” person or system |
| Context | Additional information that can be used to further evaluate the priority of allowing this user access, such as the apparent network location. |

risus, eu congue dolor nisi ac est. Suspendisse convallis magna hendrerit ante ultricies, at eleifend lorem euismod. Sed pharetra justo sit amet rutrum rhoncus. Duis eu urna mollis, feugiat risus eu, ultrices turpis. Fusce et orci ligula. Phasellus condimentum, ipsum nec fermentum semper, mauris nunc porta nisi, et vulputate dolor neque at orci. Sed eget rhoncus sapien, eu blandit lorem. Sed tempus justo quis metus porta molestie. Nulla facilisi. Nunc sed tellus nec leo tincidunt dictum nec id sem. Curabitur metus nunc, luctus ac nisi et, rhoncus gravida eros. Vivamus posuere risus ac magna luctus pharetra. Nulla facilisi.

Nullam id interdum risus. Morbi gravida odio nec justo dignissim aliquam. Aliquam tincidunt pretium nisi euismod cursus. Suspendisse id pellentesque est, ut facilisis lectus. Pellentesque in ante feugiat, tincidunt tortor quis, semper arcu. In bibendum ac enim ac luctus. Donec lacinia cursus orci vitae faucibus. Suspendisse potenti. In eget mattis ipsum. Morbi vehicula diam vitae tortor efficitur tristique. Nam tortor leo, porta at ex condimentum, placerat finibus dolor. Donec nec mauris in nulla molestie lobortis. Praesent ac dolor at augue faucibus hendrerit. Etiam vel sagittis nisl, eu accumsan nulla. In arcu odio, varius condimentum metus sed, lobortis pulvinar sem. Nunc feugiat, enim ac porttitor ornare, leo neque pretium urna, ac pharetra odio enim ac nisl.

## 1.1 Passwords

This section is about passwords.


Figure 1.1: Randomized Password

The length of the password helps the security but makes it hard to remember. Maecenas sit amet consequat diam. Phasellus molestie lorem eros, elementum consectetur purus placerat in. Fusce sed tristique risus, sit amet pellentesque erat. Donec a urna sed nisi aliquet posuere vel a nulla. Integer consequat hendrerit vulputate. Curabitur et tellus nec metus tempus tempor. In id sodales turpis. Nulla lacus est, convallis sit amet ligula non, ornare placerat tellus. Duis posuere lacus sit amet tempus scelerisque. Etiam id cursus neque. Morbi vitae ligula massa. Phasellus lacinia felis hendrerit sem commodo, id tempus ipsum imperdiet. Suspendisse eu ante mi. Sed molestie, ipsum at feugiat venenatis, magna lectus tristique ex, non semper mauris tortor sit amet massa. Aliquam eu erat turpis. Nam dignissim velit in tellus interdum, vel feugiat felis elementum.

### 1.1.1 Entropy

You may recall from high school physics that entropy has something to do with thermodynamics. Why in the world is it used to describe passwords?

Claude Shannon coined the use of the term entropy in information theory when he recognized the formula he had developed for measuring information also occurred in statistical

mechanics, where it was called entropy! He used the letter H to represent it since it was so in Boltzmann's famous H theorem, which has to do with molecules moving to equilibrium.

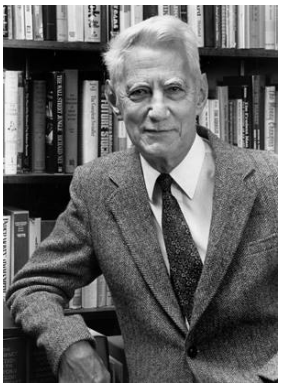

Figure 1.2: Claude Shannon

For passwords entropy denotes the uncertainty in the value of a password. Entropy of passwords is conventionally expressed in bits, which brings you back to high school math. That's right logarithms! If your alphabet consists of 26 letters, say and you require 8 letters in your password then there are $26^8$ possible passwords. That can be expressed as entropy with

$H = \log_2(26^8) = 37.6$ bits

More information is provided by NIST at `https://pages.nist.gov/800-63-3/sp800-63b.html`

Humans don't do random very well, so in reality, much of the possible space is never taken by self-selected passwords, so in practice the entropy is overstates the value.

Of course, modern computers with access to the password hash file can make quick work of this. So finding ways to prevent or throttle password guessing is important! Or, better yet, don't rely entirely on passwords!

## 1.2 Onetime

This section is about codes that can be only used once.

Of course the problem with codes that can be used just once is that there is a distribution problem.

In earlier times, this was solved by creating a codebook with two copies - one for the sender and one for the receiver.

In modern times there are time based codes, that depend on minimizing the difference between local clocks.

### 1.2.1 Pad

Here is an example of a one time pad.

```
ZDXWWW EJKAWO FECIFE WSNZIP PXPKIY URMZHI JZTLBC YLGDYJ
HTSVTV RRYYEG EXNCGA GGQVRF FHZCIB EWLGGR BZXQDQ DGGIAK
YHJYEQ TDLCQT HZBSIZ IRZDYS RBYJFZ AIRCWI UCVXTW YKPQMK
CKHVEX VXYVCS WOGAAZ OUVVON GCNEVR LMBLYB SBDCDC PCGVJX
QXAUIP PXZQIJ JIUWYH COVWMJ UZOJHL DWHPER UBSRUJ HGAAPR
CRWVHI FRNTQW AJVWRT ACAKRD OZKIIB VIQGBK IJCWHF GTTSSE
EXFIPJ KICASQ IOUQTP ZSGXGH YTYCTI BAZSTN JKMFXI RERYWE
```

Figure 1.3: One Time Pad

Vivamus eget orci fringilla augue commodo accumsan ac in eros. Donec lacinia, tellus in porta dignissim, orci arcu pellentesque neque, non dapibus ligula eros et tellus. Integer congue, tellus lacinia tristique malesuada, est odio tristique ex, eget pulvinar est sem in dui. Duis fermentum magna vel ex dignissim eleifend. Phasellus rutrum nulla non risus pellentesque

dapibus. Suspendisse bibendum ultricies sem blandit cursus. Ut ac semper nunc, ac pharetra neque. Aenean volutpat dolor vitae bibendum mollis. Nullam tincidunt consectetur tincidunt. Integer a nisi ligula.whi

# Chapter 2

# Accounts

Accounts are a not exactly the same as an identity or a user.

## 2.1 User Accounts

In an organization often users have a single account that is used for a system.

## 2.2 How to manage non personal (system) accounts

Figure 2.1: André Koot

Customer often ask me for best practices regarding management of non-personal or highly privileged accounts in the process of implementing an Identity and Access Management (IAM) solution. This is an interesting question, because in an IAM project, we try to manage all kinds of accounts, but this type of account is different from accounts that are owned by end users. This type of accounts can't directly be related to a uniquely identifiable person, nor are they the result of the 'joiner – mover - leaver' HR processes in an organization. So, how do you manage the existence of such an account?

**Types of non personal accounts**

There are Non Personal Accounts (NPA's) and Non-personal System Accounts: (NPSA's). We can identify:

- **Admin or root account**

The admin or root account of Windows and Linux or Unix servers is highly privileged system account on the respective platforms.

o It is authorized at the highest level

o It has access to every file and process running on a platform.

o The 'root' or 'Admin' has the permissions to change the behavior of their component;
o Commands can be run from it as well as react to responses of the system.
o Operational use of the account needs to be monitored continuously.

- **Superuser account** It's a business information system or application account, that looks a lot like 'root'. It is there when the system is installed, it's a system account. The Superuser has permission to modify, making it a risk critical account in an information system. Like Sap* in a Sap environment.

- **Service account**

Accounts for middleware processes like DBMS's, ESB's or other ICT components that run on top of the Windows or Linux operating systems. A special form of a non-personal account is an application account in a DBMS to give database access to an application.

- **Batch user account**

An account used by a batch job process, it is most commonly used for scheduled batch jobs, like nightly file transfers.

**NPA characteristics**

NPSA's have a few characteristics in common. They are non-personal and they are not directly connected to a person. Login with the account doesn't leave an audit trace showing which person is actually using it. And, of course, NPSA's are very powerful and so use of them should be tightly controlled.

Service and batch accounts also have a specific similarity: one typically doesn't login with such an account, these accounts are not used interactively. In most cases such an account is only used as a placeholder with some permissions to perform specific tasks, like running a webserver with the limited capability to process https-requests and write log files.

Modern IAM solutions can be implemented to facilitate provisioning of personal accounts for specific user functionality. Since non-personal accounts are not an attribute of an identity, there is not a sole user that can be connected to an NPA, so an IAM solution is not suitable to manage them.

**If not an IAM problem, then what?**

These accounts belong to the component that they manage. The Windows operating system comes with the Administrator account, Linux comes with root. You cannot install Linux without a root account. You may not by default be able to login with it (as on Ubuntu), but the account is there. So by installing an OS, you automatically get the 'God'account. There is no choice, it is the result of the change process that leads to the implementation of the OS. Such an NPSA should only be used in a controlled manner from specific processes, like an incident management process (admin may be needed to assist in a catastrophe), or the change management process (the admin permissions may be required to perform an infrastructural change).

The same is true for service accounts: when installing a middleware component, like a database management system, the account is created to enable the service, hence the name service account. Again, you have no choice. You might install the service using a 'root' –

type account, but that will result in a security violation, Thou shalt not run any service as root!

And again, for batch account the same is true again: a batch process is created as the result of a change request. The batch tasks are created to support an information system, or a business process. The batch job is created to make it possible to schedule the automatic execution of the tasks. A batch account is created to make it possible to use resources on the system.

This leads to the following conclusion:

**Non-personal accounts have to be managed in the change management process. This has the following implications:**

- The account has to be registered in the configuration management database, it is an attribute of the component that it belongs to. Admin belongs to the Active Directory. Root belongs to a linux server. The account named 'Oracle' probably belongs to an Oracle dbms instance: the dbms is a managed component and the account name is Oracle.
- The account has an owner, who is accountable for the use of the account. Admin and root belong to the manager of the ICT department. The SAP account is owned by the system owner of the SAP system
- The interactive accounts should only be used for infrastructural changes or calamities.
- The non-personal system accounts should never be used interactively for operational tasks.
- The passwords of these accounts must remain secret. They should be secured by means of an envelope procedure, a password vault, or by using a Privileged Account Management system (PAM, like CyberArk, Hitachi PAM or CA PAM to name just a few). Any use has to be related to a service management ticket (an incident or a change).

So, there you have it. Non-personal accounts must not be managed in an IAM solution, they have to be managed by the Change Management processes in an organization. Either they are owned by ICT or by the system owner who owns the information system that the account is used for. You should not manage privileged accounts in an IAM solution. And if you have to execute tasks with one of these accounts: use a Privileged Account Management system to secure it.