Task 3.1

a)

1. Biometric authentication[1]

The biometric authentication is based on the human unique biological characteristics. The most popular might be fingerprint scanner, voice recognition and iris scanner; still there are many more unique characteristics. E.g. a fingerprint scanner is found nearly on every device nowadays, like smartphones or notebooks. It is widely known that the fingerprint of every human is unique. So the fingerprint scanner creates a digital likeness of the fingerprint and authenticates the human by mapping it to the registered fingerprint image.

+ Fast authentication, only have to use one finger

+ No need to remember a password. Biometric characteristics are always accessible

- Biometric characteristics can be lost for ever (loss of hand…)

- New attack target (from information based up to personnel based)

Popular product: Apple IPhone (5s and newer)

2. Authentication through possession in addition with biometric authentication[2]

The Nymi Band also uses biometrical characteristics like the unique heartbeat rhythm of a person. It is a wearable wristband that has to be worn to use its authentication features. For the authentication the wristband measures the chosen biometrical characteristic e.g. the heartbeat rhythm of its wearer and matches it with the preregistered rhythm to authenticate the person wearing the wristband.

+ Fast and easy authentication (no input necessary)

+ Pretty safe, only the preregistered wearer can authenticate

- Wristband must always be worn and can get lost

Popular service: Nymi Band

3. TAN authentication

TAN is the transaction authentication number and is usually used in online banking. Therefore e.g. the user registered a phone number to the online bank and at the time of payment, the service sends a message to the user's phone with the TAN. This TAN needs to be entered to authorize the payment. Mostly it is a 6 character long number.

+ No possession in form of a password is needed and has to be remembered

[1] Global source for this segment: "http://searchsecurity.techtarget.com/definition/biometric-authentication"
[2] Global source for this segment: "https://nymi.com/product_overview"

- The transmission path can be intercepted

Popular service: Kreissparkasse Köln

b)[3]

Googles offers an account confirmation in 2 steps for their google accounts to users. The first step is the normal password authentication. The only restriction on the password is that it has to be at least 8 characters long. The second step provides an authentication mostly over the user's telephone. Therefore a 6 long digit code is send to the telephone via SMS, phone call or a specially designated app. A login is only possible, if both steps are performed. Alternatively the second step can also performed offline, by downloading a list of backup-codes which can be used in case the telephone is not accessible. Another option is to use a Security Key with the open standard "FIDO Universal 2nd Factor (U2F)". Usually this security key comes within an USB HID and can be added to a user's google account. To authenticate it is only necessary to pluck in the security key.

Advantages:

- Even if the password of step 1 is thieved, your account can be still save through the second authentication step
- The security of your account doesn't depends as much on the password strength, thus weakly chosen passwords don't have a high severity
- Attackers have to gain access to a physical object (telephone, security key) to pierce through the second authentication phase

Disadvantages:

- For the second authentication phase, only a 6 long digit code is send to your device. It wouldn't take long to crack this code through a brute force attack
- Attackers can also gain access to physical objects like the registered security key, or the telephone. Therefore the attack isn't based any longer on a technical, thus a physical level
- The account authentication takes more time
- More circumstances when losing the telephone

[3] Global source for this segment: "https://www.google.com/landing/2step/#tab=why-you-need-it"