FP7 – 610753

Framework Programme (FP) 7

ICT-2013.5.1 - Personalised health, active ageing, and independent living

d2) Development of mobile eHealth services to empower patients and enable patient-centric care, using mobile devices and converging software platforms

UNWIREDHealth

Deliverable 2.3
Phase 1 – Specification of eID and Security

Version	1.1
Status	Final
Date	18/05/2015
Filename	UH_D2.3_Phase 1_Specification of eID and Security_V1.1_Final_150522

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610753.

Document Information

Date of delivery	Contractual: 31/10/2014	Actual: 22/05/2015
Nature	Report	
Dissemination Level	PU = Public	

Responsible author	Ignasi Garcia-Milà	Email: igarciamila@ticsalut.cat
	Partner: TicSalut	Phone: +34 935532642

Document History				
Date	**Version**	**Author**	**Change**	**Status**
17.11.2014	0.1	Ignasi Garcia-Milà	Table of contents creation	Draft
07.01.2015	0.2	Ignasi Garcia-Milà	Legal information general update	Draft
07.01.2015	0.3	Henrik Gaunsbæk	Include Region Southern Denmark information	Draft
11.01.2014	0.4	Phil Burnside	Include Scotland information	Draft
09.02.2015	0.5	Olivier Arrondo	Technical information introduction	Draft
16.02.2015	0.6	Olivier Arrondo	Technical information update	Draft
11.03.2015	1.0	Ignasi Garcia-Milà	General review and compilation	Draft
18.05.2015	1.1	Ignasi Garcia-Milà	Review document and include modifications and comments from all regions	Final

Authors	**Name**	**Partner**
Main author	Ignasi Garcia-Milà	TicSalut
Co-authors	Olivier Arrondo	TicSalut
	Henrik Gaunsbæk	RSD
	Phil Burnside, Pam Rennie	NHS24

Keywords	Electronic Identification, Security, Information Technology Systems, Health IT, eHealth, mHealth
Abstract	The document provides an overview on the general legal framework that eHealth has regarding electronic identification and security of the IT systems. An description of the specificities of each of the procuring regions is also included.

Table of Contents

List of Tables

1 Electronic Identification

Electronic Identification (eID) is the process of unambiguously determining a person/entity's identity by using electronic means. eID is one of the tools to ensure secure access to online services and protected online content and to carry out electronic transactions in a safer way.

In Europe many Member States provide their citizens with electronic IDs via smart cards, mobile phones, or other technologies: some Member States combine an e-ID with the function of an identity card used also as a travel document, others have a citizen card to access public online services, others work with mobile devices, or a combination of card and phone.

There are different types of electronic identification. The most common is based on username and password. To access the system, the user provides credentials in a web page or app, the system checks the credentials against a reliable database and if they match then grants access to the service or content. The username and password based system has many limitations in terms of security which cannot guarantee unequivocally identifying person or entity, for this reason, we have developed electronic identification systems with higher security levels, some of them are: Digital certificates issued by reliable certification authority, stored on a computer, mobile device, or usb storage card (for example the Spanish DNIe). Biometric eID with the help of biometric reader devices. 2FA (2 factor authentication), with security tokens, mobile phones or security key.

1.1 Regulation

1.1.1 European Level

Regulations at European level, pretend to establish the condition for mutual recognition of electronic identities between EU countries, ensuring that citizens and businesses can use their electronic identity credentials to access public services, and eventually private, in other European countries and to be able to establish single electronic market trust service, ensuring electronic transactions to have the same legal value as their paper counterparts cross-borders.

There are several European Directives that have an impact to electronic identification of citizens to use and access health services.

The directives identified in the following list are the ones that are related to eID for the provision of eHealth services:

1. EU Regulation 910/2014 of the European Parliament and of the Council, dated 23 July 2014, on electronic identification and trusted services for electronic transactions on the internal market, which also repeals Directive 1999/93/CE.
   The purpose of the Regulation is to establish a clearly defined legal framework that guarantees the cross-border recognition of electronic identities, the interoperability of the electronic signature and other trusted services, such as electronic stamps or time stamps, enabling electronic communications between citizens, enterprise and the public administration and fostering trade and electronic administration.
   http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

2. Directive 1999/93/CE of the European Parliament and of the Council, dated 13 December 1999, which establishes a Community framework for electronic signatures.
   The Directive establishes a Community framework for electronic signatures and, as long as minimum requirements are met for certificates, certification services providers and electronic signature creation devices, legal effectiveness equivalent to electronic and handwritten signatures. It also provides the reference numbers for ethical standards that are widely recognized for electronic signature products.

3. Directive 2000/31/CE of the European Parliament and of the Council, dated 8 June 2000, on certain legal aspects of information society services, especially electronic commerce in the internal market.
   The purpose of the Directive is to contribute to the correct operation of the internal market, guaranteeing the free circulation of information society services among Member States.

4. Commission Decision 2000/709/CE, dated 6 November 2000, on minimum criteria to be considered by the Member States when designating bodies in accordance with section 4 of article 3 of Directive 1999/93/CE of the European Parliament and of the Council, which establishes a Community framework for electronic signatures.
   It provides the minimum criteria to be considered by the Member States when appointing national bodies responsible for evaluating the conformity of secure signature creation devices.

5. Commission Decision 2003/511/CE, dated 14 July 2003, on the publication of reference numbers for standards that are widely recognized for electronic signature products, in accordance with Directive 1999/93/CE of the European Parliament and of the Council.
   It quotes the references of three standards that are widely recognized for electronic signature products that award the presumption of conformity to the recognized electronic signature.

6. Commission Decision 2009/767/CE, dated 16 October 2009. Correction of errors in Decision 2009/767/CE, which adopts measures that enable the use of procedures by electronic channels using "one-stop shops" in accordance with Directive 2006/123/CE of the European Parliament and of the Council.
   It adopts various measures to foster electronic procedures through the use of one-stop shops.

7. Commission Decision 2010/425/UE of 28 July 2010, which amends Decision 2009/767/CE on the establishment, maintenance and publication of trusted lists of certification services providers supervised or certified by the Member States.
   It amends Decision 2009/767/CE.

8. Commission Decision 2011/130/UE of 25 February 2011, which establishes the minimum requirements for the cross-border processing of documents signed electronically by the competent authorities by virtue of Directive 2006/123/CE of the European Parliament and of the Council.
   It establishes the reference format for electronic signatures.

9. Commission Decision 2013/662/UE of 14 October 2013, which amends Decision 2009/767/CE on the establishment, maintenance and publication of trusted lists of certification services providers supervised or certified by the Member States.
   It amends Decision 2009/767/CE.

10. Decision 2014 / 148/UE of 25 February 2011, which establishes the minimum requirements for the cross-border processing of documents signed electronically by the competent authorities by virtue of Directive 2006/123/CE of the European Parliament and of the Council.
    It amends Commission Decision 2011/130/UE.

1.1.2 Country Level

1.1.2.1 United Kingdom

At a UK level, the UK Cabinet Office use ‘Verify’ which has been launched.

GOV.UK Verify is more secure than usual methods of proving who a person is because there’s no central storage of information. GOV.UK Verify uses certified companies to check it’s who the person claims to be.

Verifying the identity takes around 15 minutes, online. After that it takes less than a minute to verify the identity each time the person uses a GOV.UK service.

The certified company chosen performs some checks before verifying the identity to GOV.UK, such as questions only the person knows the answer to. The person is also asked to enter a code received on their mobile phone; this is known as 2-factor authentication.

The identity is verified by a certified company each time the person wants to use a service. The person chooses the certified company (and can choose as many as they like, and can change it at any time). They don't have an account with government.

This strictly limits the information any certified company or government has about a person: no-one has more information than the minimum to perform their function, and there is no central, vulnerable storage of information.

1.1.2.2 Scotland is using its own, but similar approach and architecture through 'myaccount'. See below. Denmark

In Denmark the level of digitization in the public sphere is very high and all public sectors and institutions follow the same regulations and build upon the same digital infrastructure. This has also meant that the Danish government, Local Government Denmark and Danish Regions have all agreed on one common electronic identification method to be used in all communication with the public sector in Denmark. The "NemID" (EasyID) was launched in the summer of 2010 and is free and accessible for all citizens.

The Danish digital signature is also known as OCES (Offentlige Certifikater til Elektroniske Services) (Public Certificates for Electronic Services) and they are based on PKI (Public Key Infrastructure). This is an infrastructure which enables authentication and confidentiality in electronic communication between two parties.

1.1.2.3 Spain

The following laws, royal decrees and resolutions from the Spanish government are the ones related to eID and applicable to the provision of eHealth services:

1. Law 59/2003 of 19 December on electronic signatures
   In Spain, this Law governs the validity of electronic signatures and the requirements that are to be met by certification services providers.

2. Law 34/2002 of 11 July on information society services and electronic commerce.
   This applies to electronic commerce and other Internet services when they are part of an economic activity.

3. Law 56/2007 of 28 December on measures for promoting the information society.
   Besides amending certain provisions of Law 59/2003, it brings in a number of regulatory innovations regarding electronic invoices and the strengthening of users' rights. It also makes necessary amendments to legislation for the promotion of the information society.

4. Law 11/2007 of 22 June on citizens' electronic access to public services.
   The Law recognizes citizens' right to maintain electronic relations with public administrations and the latter's duty to guarantee said right.

5. Royal Decree 1671/2009 of 6 November, which partially consolidates Law 11/2007 of 22 June on citizens' electronic access to public services.
   This consolidates Law 11/2007 of 22 June on citizens' electronic access to public services in the sphere of the General State Administration and public bodies linked to or dependent thereon in relation to data transmissions, electronic offices and general access points, identification and authentication, electronic registries, communications and notifications and electronic documents and copies.

6. Royal Decree 4/2010 of 8 January, which regulates the National Interoperability System.
   The purpose of this Decree is to provide criteria and recommendations on security, standardization and the storage of information, formats and applications that must be taken into account by the public administrations to ensure an adequate level of organizational, semantic and technical interoperability for the data, information and services managed in the scope of their powers and to avoid citizen discrimination on the grounds of technological preferences.

7. Royal Decree 3/2010 of 8 January, which regulates the National Security System in relation to Electronic Administration.

The purpose of this Decree is to provide the basic principles and minimum requirements for adequate information protection. It must be applied by the public administration is to ensure access to and the integrity, availability, authenticity, confidentiality, traceability and storage of the data, information and services used on the electronic media they manage when exercising their powers.

8. Resolution of 19 July 2011, handed down by the Secretariat of State for the Civil Service, which adopts the Technical Standard for the Interoperability of Electronic Documents.
   It provides the components of the electronic document, containing, where applicable, the electronic signature and metadata, as well as the structure and format required for exchanges thereof.

9. Resolution of 19 July 2011, handed down by the Secretariat of State for the Civil Service, which adopts the Technical Standard for the Interoperability of the Scanning of Documents.
   It provides the requirements for scanning documents on paper or other non-electronic media that can be scanned by photoelectric means.

10. Resolution of 19 July 2011, handed down by the Secretariat of State for the Civil Service, which adopts the Technical Standard for the Interoperability of Electronic Records.
    It provides the structure and format of the electronic record, as well as specifications for provision and forwarding services.

11. Resolution of 19 July 2011, handed down by the Secretariat of State for the Civil Service, which adopts the Technical Standard for the Interoperability of the Policy on Electronic Signatures and Certificates issued by the Administration.
    It provides the common criteria assumed by the public administration in relation to the authentication and mutual recognition of certificate-based electronic signatures and which, as such, will be developed and consolidated by the policies on certificate-based electronic signatures.

12. Resolution of 28 June 2012, handed down by the Secretariat of State for the Public Administrations, which adopts the Technical Standard for the Interoperability of Data-Brokering Protocols.
    It provides the specifications for data-brokering between public administrations and public corporations linked to or dependent thereon.

13. Resolution of 28 June 2012, handed down by the Secretariat of State for the Public Administrations, which adopts the Technical Standard for the Interoperability of Relational Data Models.
    It defines the conditions for establishing and publishing data models that are common in the Administration and those that refer to matters on the exchange of information with citizens and other administrations, as well as the associated definitions and codes, regarding publication in the Centre for Semantic Interoperability.

14. Resolution of 28 June 2012, handed down by the Secretariat of State for the Public Administrations, which adopts the Technical Standard for the Interoperability of Policies on the Processing of Electronic Documents.
    It establishes directives for defining policies on the processing of electronic documents.

15. Resolution of 19 July 2011, handed down by the Secretariat of State for the Civil Service, which adopts the Technical Standard for the Interoperability of Requirements for Connections to the Communications Network of Spanish Public Administrations.
    It provides the specifications for data-brokering between public administrations and public corporations linked to or dependent thereon.

1.1.3 Regional Level

1.1.3.1 Scotland

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see the following link for the most up to date information - http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText

A summary is also provided below:

What is myaccount?

myaccount will give people across Scotland a secure and easy way to access public services online. myaccount is designed for people who wish to use services – such as pay council tax bills or request parking permits - from Scottish public sector organisations online, rather than go into a local office or send a letter through the post.

Not everyone will want or be able to access services online themselves and alternative means continue to be available (e.g. visiting local offices in person or contacting them through the post). But for the increasing numbers of people who want to access services and undertake transactions online at a time that suits them myaccount provides a secure and convenient means to do so.

There will be many tasks that can be done online without needing to sign-in. However, when a person does need to sign in, using **myaccount gives them one username and password for secure and trusted access to all public services across Scotland**.

Here we set out how myaccount works and why it is secure.

Where can I use myaccount?

Some public services have already chosen to use myaccount and this could be seen on their websites from Spring 2014. Currently local authorities and the NHS are able to use the myaccount service, but organisations are at different stages of readiness and not all offer services online – use myaccount -immediately.

We know that there is demand to access services of other organisations such as housing associations online and the number of services that can be accessed with myaccount will be expanded in the near future.

Why set up myaccount?

We understand that when a person undertakes a transaction online they want to be confident that it is secure, that their identity is protected and that someone else cannot do it pretending to be that person.

The Scottish Government has agreed to set up myaccount with Scotland's wider public sector so people know that their transactions are secure with all public service providers. By using myaccount people will not be asked to repeatedly provide the same information every time they access a service.

Two steps to getting started on myaccount

To access services on-line using myaccount people follow two simple steps: □

Step 1: Register via **mygovscot** to create a **myaccount**. Once they have created the account they will be given a unique username and a password. □

Step 2: Use this username and password to sign-in to many of your local services online.

Once they have received their username and password they can safely sign-in to use an on-line public service. This sign-in – where they give their user name combined with their password – is a key part of protecting their identity. It will provide them with the assurance and confidence that the order or payment is attributed to them and public organisations with the confidence that they know who is accessing their service. In other words this system provides secure and trusted access to online public services.

Not all services will require a myaccount to access them e.g. if people simply want to register to receive email alerts about events in their region they will not need to sign-in. But if they want to request a special waste uplift, pay a bill or receive a delivery then it is important that both the person and the public service organisation can be confident that the transaction is actioned for the correct person.

How will this work?

If a person has visited a website of a public body – such as their local council – they will be asked to sign in.

If they already have a myaccount they will be taken to the mygovscot site where they will supply your sign-in details. Having done so they will be automatically and securely returned to the Council site to use the service they want.

If it is their first time signing in for online public services they will be invited to create a myaccount before they can sign-in. The Council or public organisations website will direct them to the mygovscot website (signin.mygovscot.org) where they can create your myaccount. mygovscot is being developed as a one stop shop where citizens, businesses and visitors in Scotland will be able to go to access online public services. The mygovscot webpage www.mygovscot.org is live and the website as a whole continues to be developed.

Trusted, secure access: Signing in with a unique myaccount username and password allows public sector organisations to verify that the person is who they say they are. It also gives them the confidence that nobody else but that person can access the account.

What information will the person provide and how is it checked?

If a person wants to create a myaccount they will be asked to provide some basic information to verify their identity and their address.

They will need to provide their full name; date of birth; gender; postal address and an e-mail address.

To verify their identity and ensure their online transactions are secure myaccount will check their name, date of birth and gender against publically available information held by the National Records of Scotland (NRS) – the public body that records births, deaths and marriages.

In the unlikely event their information cannot be matched they may also be asked for their place of birth or mother's maiden name. This would also be checked against the information held by National Records of Scotland and would not be shared any further.

When a myaccount is created a unique reference number, also provided by NRS, is attached to it. The address they have given will also be used to ensure the account is set up only for that person. It will be matched against an existing but separate register of property addresses, compiled by local authorities. Each address has its own Unique Property Reference Number.

Most importantly, these steps ensure that the account belongs to that person and only that person. It makes it easy for public services to ensure no duplicate records or fraudulent applications are created.

Increasing your 'assurance level': Once a person has created their myaccount, they will be able to access certain services right away. For some services which require a higher level of assurance or more information, they will need to provide some further information about who they are. They may be asked to provide a known fact, such as a council tax number or in a very few cases they may need to provide photographic evidence. Once they provide this additional information, they will be able to access all services that require a higher level of assurance; so you only have to do this once.

Is this an approach that is tried and tested?

myaccount builds on the approach taken when individuals apply for a card to allow concessionary travel. Up until now, application for a National Entitlement Card has been on a paper form. The information on the form is checked and held by the Improvement service who then arrange for issue of a card. (In future people will be able to apply for a Card on-line.)

By building on an existing service we know that we have a system that works and that will be cost-effective.

What happens if a person's details change? How is the information protected?

The mygovscot myaccount keeps you in control of personal information. A person will be able to check and update their details on-line – for example if they change their address.

When a person sets up a myaccount they will have the option of allowing the core information they provide – name, date of birth, gender and address – to be shared with the public service providers who use myaccount. This means that any updates they make, such as a change of address, can then be passed on securely to the public service providers they use by attaching their update to the unique reference number that goes with their account. This means they will not have to update organisations separately.

If they choose not to give consent, service providers will usually need to ask them for this information separately so that they have the information they need to give them the right service.

This approach to information sharing complies with the Data Protection Act and the Scottish Government Identity Management and Privacy Principles.

Who is providing this service?

The Scottish Government considers that the people of Scotland will prefer a public sector, not-for-profit body to be responsible for "myaccount". This contrasts with the UK Government's approach of individuals setting up an account with a private sector body.

The myaccount service was developed and is operated by the Improvement Service who, like most public bodies contract with a specialist company for ICT support. The Improvement Service is a not-for-profit publicly funded organisation that works to improve the efficiency, quality and accountability of local public services. It was originally established to support local government but now supports the public sector more widely. myaccount is funded by Scottish Government.

The Scottish Government will not have access to the information that individuals provide except where a unit of Scottish Government is a service provider, for example, the Agriculture Directorate that deals with applications from farmers for payments.

What range of services can a person access with myaccount?

Legislation allows National Records of Scotland (NRS) to share its data with local government organisations and the health service. Sharing this information is key to ensuring that Scottish residents can access their public services online in a safe and secure manner.

Many people also want to use services from housing associations and other government bodies online. To ensure that they can have the same standard of secure access to these services through myaccount the Scottish Government will bring forward legislation.

Storing a persons details securely

The Improvement Service stores details in a secure manner within Scottish, world class facilities so that there is no improper access or improper sharing. They have carried out a Privacy Impact Assessment so as to ensure their systems meet this objective. This Assessment follows guidance issued by the Information Commissioner.

The Improvement Service will only hold those personal details set out above. The Improvement Service does not and will not hold any information about the services accessed or the transactions undertaken.

1.1.3.2 Southern Denmark

The same regulation described for Denmark is applicable to the region of Southern Denmark.

1.1.3.3 Catalonia

The following laws, decrees and orders from the Government of Catalonia are the ones applicable to eID on the provision of eHealth services:

1. Order CLT/172/2014 of 14 May, which adopts the protocol for the processing of electronic documents and the archive of Generalitat de Catalunya (Government of Catalonia).
2. Decree 232/2013 of 15 October, which creates the concept of Electronic Office.
3. Decree 309/2011 of 12 April, which regulates the Board for the Promotion and Structuring of the Reform of the Administration.

4. Order GAP/459/2010 of 22 September, which adopts the protocol on interoperability.
5. Law 29/2010 of 3 August on electronic media in the public sector of Catalonia.
6. Decree 56/2009 of 7 April for the promotion and development of electronic media in the Autonomous Administration of Catalonia.

1.2 Mobile Identification

Mobile Identification is an electronic identification method, in which the identification credentials are provided by/through a mobile device. The credentials can be provided by biometric readers, through an app that stores it, using a digital certificate stored on the device or directly typing in the app or web page login and password.

Mobile Identification provides a much higher security level than a username and password based system because to authenticate the user must use his mobile phone (usually a very personal device). In addition to the credentials supplied, mobile device are associated with a unique electronic identifier, and can provide the identification system data of the network to which it is connected and geolocation. Biometric readers like face recognition systems by camera and fingerprint reader also provide enhanced security.

1.2.1.1 Scotland

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see the following link for the most up to date information- http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText (also see section 1.1.3.1 above)

1.2.1.2 Southern Denmark

There is no specific Mobile Identification used in the Region of Southern Denmark. All public instances in Denmark are required to use the national eID 'Nem ID' regardless of whether a service is for normal website or for mobile use.

Read more about 'NemID' in section 1.3.9.2 of this document.

To facilitate easy mobile access, some services in Denmark - like the secure mail system eBoks – has set up their app so that you have to sign on with NemID to the regular website and create a personal mobile username and password linked to your account (based on the unique personal social security number). The mobile password then gives access to the electronic inbox in the mobile app.

1.2.1.3 Catalonia

1.2.1.3.1 MobileID

In November 2013 Barcelona City Council launched the idBCN application for smartphones, which enables citizens to communicate with the local administration and carry out some administrative procedures. In February 2014 the system changed his name the actual name MobileId, and incremented the number of available services. The system is based on an APP that store encrypted credentials. To be able to obtain the service you first have to fiscally show a valid Id at the Authorized Citizen Advice Office or to have a valid electronic certificate. At this moment the number of available services is very limited.

1.2.1.3.2 User/password

User can have access to a number of public electronic services through the mobile or full version of the web service such as:

Tax agency

Health Records in Catalonia (la meva salut)

Barcelona Provincial Council tax related procedures

1.2.1.3.3 Cl@vePin

Cl@ve-Pin is a two factor authentication system based on a User/Password as first factor and a Pin send by SMS valid for limited time as the second authentication factor. With this system the Spanish citizens can access a different services, information and procedures provided by the Ministry of Treasure and Public Administrations of Spain, trough mobile version of web pages or trough specific apps, for example:

Agencia Tributaria
With this app, users can have access to tax related procedures that don't require a digital certificate.

Seg-Social Cita Previa
This app let the citizen make an appointment to carry out procedures in their offices without waiting.

A growing number of apps to communicate with public services, can be found on Appstore, Google Play and some in Windows Phone Store

1.3 Technologies available

1.3.1 Login/Password (Local database)

It's the most common eID authentication method. To have access to a protected service or content the user must provide a login and password, if the credentials match the ones stored in a database, the system grants the user the access to the service or content. The user must be registered prior to access the service or protected content. The registration process can be offline (for example you register physically at some office showing an id), online, filling out some form or a mix of online and offline.

1.3.2 Biometric Identification

Biometrics eID is an authentication by which a user authentication information is generated by digitizing measurements of a physiological or behavioral characteristic. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic.

Common types of biometrics include:

- **Fingerprint / Palmprint**: recognizes the physical structure of a person's fingerprint / palmprint, e.g. the minutiae points that include bifurcations and ridge endings
- **Hand geometry**: recognizes the shape of a person's hand
- **Retina Scan**: Recognizes the patterns of the blood vessels on the backside of the eyeball
- **Iris Scan**: Recognizes the unique patterns, rings, and corona in the iris, which is the colored portion of the eye
- **Signature dynamics**: Recognizes the electrical signals, pressure used, slant of the pen, the amount of time and patterns captured in creating a signature
- **Keyboard dynamics**: Recognizes the electrical signals when a person types a certain phrase on a keyboard, such as speed and movement
- **Voice print**: Recognizes the subtle difference in people's speech sounds and patterns
- **Facial scan**: Recognizes the attributes of a person's face, bone structure, nose ridges, and eye widths

Biometric eID always require a hardware sensor/reader. Almost all phones, mobile devices and laptops have camera and it's increasingly common to find mobile devices with built-in fingerprint readers.
This method is frequently used in combination with login/ password method to offer two factor authentication.

1.3.3 Near Field Communication (NFC)

NFC is a short-range wireless communication technology that enables the exchange of data between devices. NFC Smart Card, Phone and mobile devices NFC enabled are already present in our daily lives and used for payments, access control, transportation, etc. To authenticate the user just place NFC card close to the reader and the access to the service or contents is granted. Spanish users can have access to a secured mobile service just placing new DNI-e 3.0 close to the NFC enabled mobile device when prompted for authentication (DNI-e 3.0 enabled services). It can also be used in combination with a pin o user/password authentication to provide two factor authentication.

1.3.4 Third party authentication

This system is the basis of electronic authentication today. Instead of managing a local database for each service or protected content, systems delegate credentials verification to a reliable authority that provides the authentication service.

When the user accesses a protected service or content, the user is prompted credentials (using different methods, login / password, certificate, etc), the system then verify the credentials with a trusted authority (either an official certification authority or a trusted private company, like Microsoft, FaceBook, Google, Twitter etc).

This authentication system is more efficient for both, users and service providers. Users can consolidate their electronic identity and thus avoids having to register for each of the services they need to access and service providers avoid having to develop and maintain a system of electronic authentication for each service.

In order to ensure interoperability, credential exchange standards have been developed, the most common are:

- OpenID (Microsoft, Google, etc)
- OAUTH (Twitter, Facebook)
- SAML (Cl@ve).

1.3.5 Digital certificates

A digital certificate is an eID that allows a person, computer, mobile device or organization to exchange information securely over the Internet using the public key infrastructure (PKI). A digital certificate provides identifying information, is forgery resistant and can be verified because it was issued by an official, trusted agency/ Authority. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that an identification system or recipient can verify that the certificate is real.

To provide evidence that a certificate is genuine and valid, it is digitally signed by a root certificate belonging to a trusted certificate authority. Operating systems, browsers and mobile devices maintain lists of trusted CA root certificates so they can easily verify certificates that the CAs have issued and signed. Digital certificates can be stored on:

- Brower store/ Computer
- Physical store (pen drive, sdcard, NFC card)
- An id Card
- A mobile phone/ app

1.3.6 Two-factor authentication 2FA

Two-factor authentication is an authentication method that adds a second level of security to the login/password method. When the user have to enter only a username and a password, that's considered a single-factor authentication. 2FA requires the user to have two out of three types of credentials before being able to access an account. The three types are:

- Something the user know, such as a Personal Identification Number (PIN), password, or a pattern.
- Something the user have, such as an id card, digital certificate, phone, security token or security key.
- Something the user is, such as a biometric like a fingerprint or voice print.

Common second authentication factors are:

- **Security token**
  Either hardware or software that randomly generates a security code at a given time interval synched with the authentication system. Usually a device similar to an usb dongle with a screen that displays the security code. RSA SecureID

- **Security card keys**
  Very common to validate bank transactions. A card with a set of coordinates, the authentication system ask the user for a random coordinate. Every card has a unique set of coordinates.
- **Security key**
  Hardware that stores a digital certificate. When prompted the user must connect the device to the computer or mobile device and then press a physical button on the key, the key then communicate with the authentication system and send the info only if the system authenticates itself (eliminates phishing). Google security key
- **SMS**
  Every time the user authenticates with login/ password, the system send a PIN or security code by SMS to the user's previously registered phone, once received, the user enters this pin to as the second factor.
- **Email verification**
  Similar to SMS the user receive the PIN or security code to a previously registered email address.
- Biometric Identification (View Biometric Identification above)

Risk Based 2FA

If the user accesses a service from a different location than he usually does, logic integrated in the authentication system detects the issue and ask for a second factor authentication.

1.3.7 STORK PROJECT (Secure idenTity acrOss boRders linked)

Stork project is was and European Commission pilot project launched in May 2008 to ensure cross-border recognition of national electronic identity (eID) systems and enable easy access to public services in 13 Member States (at the first moment, now 19 Member states).
The project conducted several eID pilots in six areas to test interoperability and security with different Member States involved in each case, and trying to admit as many foreign credentials as possible.

The project main goal is to make it easier for citizens to access online public services across borders by implementing Europe-wide interoperable cross border platforms for the mutual recognition of national electronic identity (eID) between participating countries. It will do so by:
Developing common rules and specifications to assist for the mutual recognition of eIDs across national borders.
Testing with real users, in real life environments (pilots), secure and easy-to-use eID solutions for citizens and businesses;
Interacting with other EU initiatives to maximize the usefulness and the reutilization of eID services.

At the technical level one of the principles of the project has been to design and deploy a solution based on open source and open standards to allow for an easy integration of Member States and business in the future. Therefore, STORK core technologies are based on Java and SAML2.0 federation of identities. For Service Providers also php and .net technologies are supported.

Project STORK ended successfully and project STORK2.0 will continue the project by building on the results of STORK, establishing interoperability of different approaches at national and EU level, eID for persons, eID for legal entities and the facility to mandate.
STORK 2.0 will be a step forward towards the creation of a fully operational framework and infrastructure for electronic identities and authentication in the EU. It does so through:

- Exploiting experiences from four cross border, cross sector pilots with real impact demonstrating the use and societal impact of the cross border, cross sector infrastructure developed
- Common specifications and building blocks for interoperable legal identities and mandates, on top of the interoperability infrastructure developed in STORK, following privacy rules (and advice from Art.29 Working Party) and enabling secure operation
- Solving within the scope of the pilots legal issues such as privacy/data protection, liability, and different National regimes
- An update of the QAA model to include attributes, legal entities and mandate agreements
- eID packaged as a service for governments and businesses including a cost model and promoting the business take-up of STORK
- Addressing eID governance issues through the requirements for an accreditation body

- Investigating and promoting standardization in the area of eID using STORK 2.0 solutions
- A knowledge repository and awareness of the STORK 2.0 infrastructure and its potential societal impact on business processes

More information:
https://www.eid-stork.eu/
https://www.eid-stork2.eu/

1.3.8 FIDO ALLIANCE (Fast IDentity Online)

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO authentication is stronger, private, and easier to use when authenticating to online services. Fido alliance was created to develop the FIDO standard specifications and FIDO-enabled devices.

The FIDO standard supports a full range of technologies, including biometrics such as fingerprint scanners, voice and facial recognition, as well as existing authentication solutions and communications standards, such as Trusted Platform Modules (TPM), USB Security Tokens, Near Field Communication (NFC), One Time Passwords (OTP) and many other existing and future technology options. The open protocol is designed to be extensible and to accommodate future innovation, as well as protect existing investments. The FIDO protocol allows the interaction of technologies within a single infrastructure, enabling security options to be tailored to the distinct needs of each user and organization.

UAF/U2F FIDO alliance authentication protocols.
This authentication methods pretend to eliminate the need of a password using hardware devices/ sensors to provide credentials.
Passwordless UX (UAF)

User carries client device with UAF stack installed
User presents a local biometric or PIN
Website can choose whether to retain password

The passwordless FIDO experience is supported by the Universal Authentication Framework (UAF) protocol. In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user.

Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN.

Second Factor UX (U2F)

User carries U2F device with built-in support in web browsers
User presents U2F device
Website can simplify password (e.g. - 4 digit pin)

The second factor FIDO experience is supported by the Universal Second Factor (U2F) protocol. This experience allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login. The user logs in with a username and password as before. The service can also prompt the user to present a second factor device at any time it chooses. The strong second factor allows the service to simplify its passwords (e.g. 4–digit PIN) without compromising security.

During registration and authentication, the user presents the second factor by simply pressing a button on a USB device or tapping over NFC. The user can use their FIDO U2F device across all online services that support the protocol leveraging built–in support in web browsers.

Fido v1.0 final complete specifications can be downloaded here: https://fidoalliance.org/specifications/download

In October 2014 Google announced that they are strengthening their 2-Step Verification by offering support for Security Key, a FIDO Ready™ U2F compliant physical USB second factor device that offers a simpler, stronger alternative to today's six digit one-time passcodes (OTP). Google's new Security Key solution offers even more protection for their most security-sensitive users. Rather than typing a code, the user just inserts a Security Key into their computer's USB port and taps it when prompted in the Google Chrome browser. When signing into a Google Account this way, users can be assured that their second factor cannot be phished, because Security Key doesn't provide its cryptographic signature when a fake site is attempting to impersonate a Google sign-in page in Chrome. Chrome incorporates the open FIDO Universal 2nd Factor (U2F) protocol, so other websites with account login systems can now build support for FIDO U2F into their web applications and instantly enable this experience for their users who run Chrome.

In February 2015 Microsoft announced it will ship a password replacement solution in Windows 10, and plans to support FIDO authentication with Windows 10 sign-in, Azure Active Directory, and major SaaS services. Future plans will showcase FIDO authentication in Windows 10 Active Directory integration for on-premise scenarios and Microsoft Account integration for Microsoft consumer services, such as Outlook.com and OneDrive.

1.3.9 eID solutions

1.3.9.1 Scotland

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see the following link for the most up to date information- http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText (also see section 1.1.3.1 above)

1.3.9.2 Southern Denmark

In 2010 the Danish government, Local Government Denmark and Danish Regions have all agreed on one common electronic identification method to be used in all communication with the public sector in Denmark; the "NemID" (EasyID), which is now the only official digital signature for public digital services in Denmark. The NemID is a personal and unique so-called Digital Signature, which is free and accessible for all citizens in Denmark (including those who live abroad but still need to communicate with Danish public authorities).

Since the launch in 2010 the use of NemID has rooted itself firmly in the Danish society – largely 'pushed' by the fact that many public services are now ONLY available online (tax services, application for admission to educational institutions, appointment letters from hospitals among others). Today more than 60.000.000 NemID transactions has been performed and more than 4.3 million personal IDs have been issued. The average monthly number of transactions – not including use with private sector such as banks – is at 13 million. (Statistic come from the NemID website that publishes statistics every quarter. These numbers are from October 2014).

About NemID:

NemID is the official Danish digital signature since 2010. The NemID can be used as a secure login regardless of where you use it - whether you are accessing your online banking service or the local public authorities' self-service or whether you are checking your insurance or retrieving your tax return form from the Danish tax authorities, SKAT.

The NemID can be used on all computers as it doesn't need any form of software installed on the computer. NemID consists of a user ID, a password which only you know and a small physical code card containing codes (one-time passwords). When you log on, you first enter your user ID and password and then a code from your code card. Therefore, NemID offers strong protection against intruders and hackers

You choose your own user ID and password – which you must commit to memory – and the code card is a small card about the size of a credit card which you need to look after carefully.

NemID was originally based on Java Applet technology. Because of limitations in this technology, the Danish Agency for Digitisation launched a new version of NemID based on JavaScript technology in July 2014, which enabled secure mobile access to NemID-based digital services.

NemID for business

NemID employee certificate is a further development of the employee digital signature that has been around in Denmark since 2002. The employee certificate allows someone to identify himself as an employee of a particular company or organization when:

- Communicating with the public authorities on behalf of the company
- Signing documents online
- Accessing information from a public authority

The employee certificate can also be used to access internal IT systems, or to send or receive secure e-mails that are encrypted and signed using a digital signature.

There are two types of employee certificate;

- NemID employee certificate with a key file that corresponds to your employee digital signature (the previously used national standard for digital security). This is a software solution where the certificate is installed on the employee's computer.
- NemID employee certificate with a code card, which is like personal NemID. This is a code card solution where the certificate is deployed on a central server at Nets DanID.

The Region of Southern Denmark doesn't have its own eID solution but uses the national solution NemID. In addition, the EHR information available for citizens in the region isn't on a regional platform but on the national website www.sundhed.dk (www.health.dk) where all citizens can view their EHR in the "e-Journal" using their NemID. In the "e-journal" (e-health record) citizens, GPs, specialised doctors as well as health care personnel across sectors can find clinical data about treatments, examination results and critical patient information from the public hospitals (if the treatment or examination has occurred within the last 10 years).

The PHR in RSD, the Shared Care Platform, also uses the NemID to let patients access their information. To facilitate access to the portal on tablets, the patients can sign in via a normal browser first and then create a personal user name and password to be used on their mobile devices – but as this is not as secure as using the NemID, and it is up to each user to decide if they want to use this solution or just the web browser with NemID.

1.3.9.3 Catalonia

Login/ Password.
It's a general common method implemented to have access services and protected content.
With this authentication method, individuals, legal entities and organizations can access different content related to them that goes from tax information to health records.

Digital Certificates

With this authentication method, individuals can access different content related to them that goes from tax information to health records. With digital certificates, users can also perform different procedures, all tax related procedures, access to health records. It's also used to authenticate professionals, for example in healthcare professionals need a digital certificate to make a national healthcare system prescription.

The following table shows the list of principal certificates accepted in Catalonia and the accreditation profiles with which they can be used.

Table 1. List of accepted Digital certificates for electronic public services identification

Accepted Digital Certificates		
Certificate Issuer	**Certificate**	**Accreditation profiles**
Consorcio de Administración Abierta de Cataluña	*idCAT*	Individual
Dirección General de Policía	*eDNI*	Individual
Ceres - Fábrica Nacional de Moneda y Timbre	*Certificado de identidad de persona física*	Individual
	Certificado de persona jurídica en el ámbito tributario	Legal entity
Autoridad de Certificación de la	*Certificado de ciudadano*	Individual

Comunidad Valenciana		
Izenpe	*Certificado de ciudadano*	Individual
Camerfirma	*Certificado de pertenencia a entidad*	Individual related to an organization without representational capacity. Individual
	Certificado de representante	Individual related to an organization with legal representation capacity.
	Certificado de persona jurídica	Legal entity
Firma Profesional	*Certificado corporativo de persona física*	Individual related to an organization without legal representation capacity. Individual
	Certificado corporativo de representante legal	Individual related to an organization with legal representation capacity.
	Certificado corporativo de persona jurídica	Legal entity
	Certificado corporativo de colegiado	Individual affiliated to a professional group.
Associación Nacional de Fabricantes - Autoridad de Certificación	*Clase 2 de persona física*	Individual
	Clase 2 de persona jurídica	Legal entity
Autoridad de Certificación de la Abogacía	*Certificado reconocido de colegiado*	Individual affiliated to a professional group. Individual
	Certificado corporativo reconocido de persona jurídica	Legal entity
Agencia Notarial de Certificación	*Certificados notariales personales*	Individual
	Certificados notariales corporativos de corporaciones de derecho público	Individual related to an organization without legal representation capacity. Individual
	Certificados para empleados de notarías y colegios notariales	Individual affiliated to a professional group. Individual
	Certificados notariales corporativos de representación	Individual related to an organization with legal representation capacity.
AC Organización Médica Colegial de España	*Certificado reconocido corporativo de colegiado*	Individual affiliated to a professional group. Individual
HealthSign	*Certificado reconocido de colegiado*	Individual affiliated to a professional group. Individual

Complete updated list can be found on this link: http://tramits.gencat.cat/en/sobre-la-oficina/tramitacio-en-linia/certificacio-digital/certificats-acceptats/

With this authentication method, individuals can access different content related to them that goes from tax information to health records. With digital certificates, users can also perform different procedures, all tax related procedures, access to health records

Cl@ve

Cl@ve is the Spanish common authentication platform to access all public electronic services. Cl@ve was launched on November 19 of 2014 to unify and simply the citizens electronic access to public services. The users can communicate with public sector with one single set of credentials, and when an increased security level is needed the user receive a PIN by SMS as a second factor authentication.

To be able to use Cl@ve a previous registration is required, either online if the user have a valid digital certificate or physically in different government offices.

Cl@ve permanente: The user access services with a set of credentials (user/password) guarded by the user.
Cl@ve PIN: The user access the system with a user, and a dynamic password result of the combination of a fixed password plus a PIN received by SMS when the user authenticates the system. This PIN is valid just for a few hours, and expires every day at 00:00.

It possible to use Cl@ve to access:

Tesorería de la Seguridad Social (Consultas y trámites frecuentes incluidos en Tu Seguridad Social)
Tax Agency
Dirección General de Tráfico (Driving license points and fines)
Ministerio del Interior (Diferent procedures)

According the Cl@ve launch press release (in Spanish) by the end of 2015 all the public sector electronic services will be available using Cl@ve Authentication.

DNI-e 3.0

On January 12, 2015, The Interior Minister Jorge Fernandez Diaz, introduced the new DNI-e 3.0 which has a new, faster and with more storage capacity, chip. The eID is also incorporates NFC (Near Field Communication) and can seamlessly communicated with NFC enabled devices to authenticate the user when accessing protected services. It also includes new security measures and gives electronic signatures the same legal validity as a handwritten signature.

Launch of the new DNIe 3.0 is performed in Lleida city and its pilot implementation will be progressively extended to the rest of the Spanish territory.

Failure of DNIe as eID.

DNIe 1.0/2.0 is available in Spain for more than ten years now, with a chip that stored the Id information, the users signature and fingerprint, a digital certificate and digital signature with authentication purpose. The problem is that citizen don't use the DNIe as eID very often, and to use it the user have to remember a PIN received when the DNIe is issued at the Police (User can change this PIN, but rarely does),user end up forgetting the PIN. Another stopper is the need of a card reader, a very cheap piece of hardware that almost no-one have a home.

DNI-e 3.0 incorporates NFC technology and dismiss the use of the PIN, eliminating the barriers that produced the failure of prior version of DNIe.

To be able to authenticate with DNI-e 3.0 the user need to have an NFC enabled device, most of midrange and high end mobile devices incorporate this technology today. When the user is accessing a protected service, when prompted he will be able to authenticate just by placing the DNI-e 3.0 in the back of the phone or mobile device. In combination with username/ password authentication it becomes a 2FA method with a high security level.

1.3.10 Mobile eID solutions

1.3.10.1 Scotland

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see the following link for the most up to date information- http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText (also see section 1.1.3.1 above)

1.3.10.2 Southern Denmark

The official eID solution (NemID) was in the beginning not programmed to run on mobile devices as it used Java Applet technology. In July 2014 the Danish Agency for Digitisation launched a new version of NemID based on JavaScript technology which enabled secure mobile access to NemID-based digital services.

This means that there are no other mobile eID solutions developed in Denmark or RSD.

Because of the delay of four years for mobile use of NemID since the introduction in 2010, many private companies such as banks have created individual mobile apps to allow users to have mobile access to services.

Some public authorities (like the national tax agency and the secure public mail system that almost all public institutions including hospitals use to send communication such as appointment letters and notifications to citizens) allow users to gain mobile access to their services by asking them to sign in with NemID via a normal browser first and then create a personal user name and password to be used on their mobile devices – but as this is not as secure as using the NemID, it has been up to each user to decide if they wanted to use this solution or just use the web browser with NemID.

One issue with having NemID available for mobile sign on is that the majority of the websites with digital self-service solutions are not optimized for mobile devices and thus don't provide for a very satisfying user experiences. This is something that most Danish public institutions are now working on improving as it is part of the national eGovernment and Digital Self-Service Strategy for 2013-2020.

1.3.10.3 Catalonia

MobileId

The MobileID digital identity system allows citizens to identify themselves remotely and securely by means of a digital ID in their mobile phone. It is based on a Register of Mobile Digital Identities that makes it possible to associate a mobile phone number with any citizen who wishes to have this new form of digital accreditation.

Any user who has a smartphone connected to the Internet (via a data line or WiFi) will be able to request and use their MobileID digital ID through an application available for iPhone and Android.

The technical system supporting this ID meets national and international legal and technical standards that are transparent to citizens, who interact only with their mobile phone application. This system can be used to access websites securely, as well as services delivered through other channels, for example, by telephone or face-to-face.

Barcelona is the first city to introduce a system of this kind for its citizens and is doing so to provide access to online municipal services.

1.4 Future solutions

1.4.1.1 Scotland

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see - http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText

1.4.1.2 Southern Denmark

Further use of NemID improving the mobile experience across the board of available digital solutions and services from public authorities including healthcare.

1.4.1.3 Catalonia

Catalonia is organising several pilots to validate technology to access clinical information available at PHR.

SIM based authentication

The SIM card contains a certificate that allows the authentication of the user accessing a specific service. The service receives a token according the user authenticated.

Mobile Connect

Mobile Connect is a new authentication solution designed to enable customers to use their mobile phone as a key to securely and easily log on to any digital service regardless of the device or network connection used. The solution is based on a highly-secure platform that uses the SIM card – which is already recognized for its inherent security - to validate entry into secure digital services. Mobile Connect is designed to respond specifically to the needs of consumers who increasingly have to manage multiple online or cloud-based accounts, each with different login names and passwords.

When accessing a Mobile Connect enabled service/content the user will enter an id (his unique id) on the web page and then he will receive a prompt in his mobile phone, to authenticate the user just have to respond the prompt, tapping ok for example.

A pilot project run through the Mobile Word Capital initiative in Barcelona and involving the GSMA, Orange, Morpho and the Catalonian healthcare service has also agreed to test the authentication mechanisms in a live environment.

Biometric authentication

The European co-funded project PIDaaS (Private Identity as a service) will implement a pilot to access the PHR system in Catalonia using voice and face recognition. (www.pidaas.eu)

DNI-nb

Cloud based DNI is a system integrated in Cl@ve, that will allow user to electronically sign document with a cloud based electronic signature. The system is under development and it will be available during 2015. Certificates for cloud based electronic signature will be issued by “Dirección General de la Policía” and will be guarded by Administration. To be able to use the certificates the only requirement will be and internet enabled device, no extra hardware or peripheral devices.

1.5 Review of solutions

Table 2. Review of eID solutions

Authentication Name	Brief Description	Security	Pros	Cons
Login/ Password	The user provides a set of credentials that must match the ones stored in a local database or a trusted authentication provider.	Low	Simple, very common, cheap to implement	Security depends on password policies and the ability of the authentication system to detect/ block brute force attacks. The user must remember his password, can be a problem if service is not used very often.
Biometric	Authentication information is generated in real time by digitizing measurements of a physiological or behavioral characteristic.	High	Secure, password-less, simple	Requires extra hardware to read physiological or behavioral characteristic. Expensive. Biometric readers can be tricked.
NFC	Authentication based on a physical card or tag, when prompted the user just have to place the card close to the back of the phone or mobile device and the access to the service is automatically granted.	Medium	Secure, password-less, simple	Requires NFC card and NFC enabled phone or mobile device.
Digital Certificates	The user provides a digital certificate issued by a trusted authority.	High	Secure, password-less, simple	The user must follow a process to obtain the certificate.
2FA	Sequential combination of 2 or more method to authenticate.	High	Depends on combined methods.	Depends on combined methods.
2FA FIDO	Sequential combination of 2 or more method to authenticate, plus service/ content provider authentication , (avoid phishing)	High	Secure, password-less, interoperability	Requires FIDO Ready Hardware

2 Security on Health IT systems

Health IT systems, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the system. This vulnerability increases as IT Systems and medical devices are increasingly "connected" to the Internet, hospital networks, and to other medical devices.

To mitigate and manage cybersecurity threats, many measures are commonly implemented. Authentication, Encrypted data connections (SSL), System access log, by user, by professional, when, where, how (Computer, Mobile device etc), Electronic certification of servers and service providers to avoid phishing.

2.1 Regulation

Security requirements for IT Health systems, medical apps and electronic medical devices are a mix of overlapping (sometimes outdated) general directives with very little attention on security, specific updated directives are still under development. The exception is the security requirements in the EN 62304 harmonized standard for Medical device software — Software life-cycle processes, with applies to medical devices.

One of the main aspects of IT Health systems security is the data protections and EU General Data Protection Regulation is still under negotiation, the forecast is that it will be finalized during 2015. Currently, manufacturers and software developers are applying country level regulations.

NIS (Network and Information Security Directive) may also apply. IT Health Care systems, mobile devices and apps will all be connected through the cloud and therefore will fall under the scope of the directive.

2.1.1 European Level

The directives identified in the following list are the ones related to the definition of security issues for the provision of eHealth services:

1. Directive 2011/24/UE of the European Parliament and of the Council, dated 9 March 2011, on the application of patients' rights in cross-border healthcare.
   The directive establishes a general framework for clarifying patients' rights regarding their access to cross-border healthcare and the corresponding reimbursement; guaranteeing the quality and safety of the care they receive in another Member State of the EU and fostering cooperation in healthcare among the Member States.

2. Regulation (CE) 883/2004 of the European Parliament and of the Council of 29 April 2005 on the coordination of Social Security systems.
   The Regulation coordinates Social Security systems to provide free circulation for citizens in the European Union.

3. Regulation (CE) 987/2009 of the European Parliament and of the Council of 16 September 2009, which adopts the rules for applying Regulation (CE) 883/2004 on the coordination of Social Security systems.
   The Regulation also coordinates Social Security systems to provide free circulation for citizens in the European Union, specifying the forms of application that must guarantee the speed and effectiveness of the benefits that are provided despite the differences in national Social Security systems.

4. Regulation (UE) 1231/2010 of the European Parliament and of the Council of 24 November 2010, which extends the application of Regulation (CE) 883/2004 and Regulation (CE) 987/2009 to the nationals of third-party countries who, due only to their nationality, are not covered by said countries.
   It extends the personal scope of Regulation (CE) 883/2004 and Regulation (CE) 987/2009 to nationals of third-party countries that are in a cross-border situation and are not covered by said Regulations as a result of their nationality.

2.1.2 Country Level

2.1.2.1 Denmark

In 2010, the Danish government decided that government institutions must follow the international standard, ISO/IEC 27001, when an update and a translation into Danish of the standard had been completed. The update was published in January 2014 therefore ISO/IEC 27001 now has replaced DS 484 as the national standard for information security management.

DS 484 was previously the security standard in government institutions and was based on the international standard ISO/IEC 27002 "Code of practice for information security management", modified to suit Danish conditions. With the introduction of this standard, IT security management in all ministerial areas was structured according to a common concept.

Activities to develop, maintain and inform users about the requirements of the standard are handled by the Ministry of Finance, represented by the Agency for Digitisation, in collaboration with other authorities in the public sector. In addition, the Agency for Digitisation is in charge of developing tools, templates, seminars and workshops to support implementation and maintenance of the standard. However, it is the task and responsibility of each individual institution to organise security work in their own organisation.

Security Forum

To support collaboration about information security across the government sector, the Government IT Council has established the Government Information Security Forum (GISF), in which about 30 government institutions participate. The Forum meets 4-6 times a year and is charged with the following tasks:

- to contribute to exchanging experience about the use of the standard,
- to follow the general development of information security management by public authorities, and propose joint initiatives that may strengthen information security,
- to determine the best practice and make proposals on how to improve paradigms and the activities carried out by the Agency for Digitisation,
- Starting from the tasks and purposes above, to support professional coordination between authorities and contribute to achieving agreement about the requirements for information security in the public sector.

The Agency for Digitisation holds the chairmanship of GISF and provides secretarial assistance. The present portal is operated by the Secretariat and aims to contribute to the exchange of experience, distributing information material, creating awareness of courses etc. and supporting administration of the Forum.

OIO architecture framework

The OIO architecture framework is the common public framework for working with architecture and standards. The framework comprises principles, methods, standards for documentation and classification of architecture work, and also a number of tools.

The OIO architecture framework - also known as OIO EA - is an "umbrella" for collecting a range of elements that help stakeholders in an architecture project.

For each step in the OIO EA method, there is a description of objectives, stakeholders, input, output, method, example, good advice and links.

The method supports various types of architecture projects (scenarios).

The framework works in the same way as a bookcase, keeping track of documentation and making it easier to retrieve and share knowledge.

- The OIO architecture framework is based on the Enterprise Architecture (EA) concept, which incorporates both business and IT architecture, and covers both the individual organisation and a cross-organisational perspective.
- The core of the OIO architecture framework is the OIO EA method and the OIO EA architecture bookcase, which provide an overall framework for architectural work and the documentation of this.
- The OIO EA framework is intended to ensure coherence across the various OIO methods, guidelines and tools, e.g. the OIO catalogue of technology standards, OIOXML data standards (known as the InfoStructure Base), OIO web services, etc.

Open standards

In September 2007, the Danish Government, Local Government Denmark and Danish Regions concluded an agreement on the use of mandatory open standards for software in the public sector. The agreement implies that all public authorities, from 1 January 2008, are to use seven sets of open standards for new IT solutions. The agreement also requires the authorities to be able to receive text documents in two open document standards.

From 1 January 2008, it will be mandatory for all public authorities to use a number of open standards for all new public IT solutions. This implies that public authorities are required to make sure that future IT solutions are based on, or support, these mandatory open standards. This is the result of an agreement concluded by the Government with Danish Regions and Local Government Denmark following discussions with the IT spokesmen of the political parties.

The agreement on introducing open standards in the public sector has been made for the purpose of promoting a competitive market for software and to enable public IT systems to exchange information across systems irrespective of the choice of software.

It is part of the agreement that the introduction of mandatory open standards should not involve increased costs to the public sector. In the light of this, an economic impact analysis will be made for each potential mandatory set of open standards. This analysis will ensure that the introduction of each individual standard is optimal from a socioeconomic viewpoint.

The following set of mandatory open standards will enter into force on 1 January 2008:

- Standards for data exchange between public authorities (OIOXML)
- Standards for electronic file and document handling (FESD)
- Standards for electronic procurement in the public sector (OIOUBL)
- Standards for digital signatures (OCES)
- Standards for public websites / homepages and accessibility
- Standards for IT security (DS484 - only for the government sector)
- Standards for document exchange (ODF/OOXML)

The Government, Local Government Denmark and Danish Regions have agreed to continue focusing on standardisation and the use of open standards. This will contribute to ensuring cohesion in the public sector, with a software market supporting competition, innovation and diversity, which will be of benefit to the development of e-government.

The right to privacy is a constitutional right for every Danish citizen regulated, among others, by the following acts:

- Act No. 429 of 31st May 2000 relating to the processing of personal data (Persondataloven) with accompanying regulations.
- Act No. 913 of 13th July 2010 relating to personal health filing systems and the processing of personal health data, relating to patients' rights, health personnel etc. (Sundhedsloven) with accompanying regulations.

Several laws regulate the security and privacy of health care data collected in the Danish health care system:

- Act No. 429 of 31st May 2000 relating to the processing of personal data (Persondataloven) with accompanying regulations.
- Act No. 913 of 13th July 2010 relating to personal health data filing systems and the processing of personal health data, relating to patients' rights, health personnel etc. (Sundhedsloven) with accompanying regulations.
- Act No. 1093 of 05th of July 2013 relating to responsibility of social care (Serviceloven) with accompanying regulations.
- Act No. 1350 of 17th December 2008 relating to the authorisation of health personnel and healthcare organisations (Autorisationsloven) with accompanying regulations.
- Act No. 24 of 21st January 2009 relating to patients' right to complaint and compensation (Patientforsikringsloven) with accompanying regulations.
- Executive order No. 528 of 15th June 2000 relating to security measures for the protection of person-identifiable healthcare information in the public healthcare system (Sikkerhedsbekendtgørelsen) with accompanying regulations.
- 'IT-sikkerhedsvejledning for sygehuse' of 17th July 2002 relating to data security in the healthcare industry.

Control Authority

The Danish control authorities are:

- Datatilsynet, The Danish Data Inspectorate See http://www.datatilsynet.dk
- Sundhedsstyrelsen, The Danish Board of Health Supervision See http://www.sst.dk
- Lægemiddelstyrelsen, Danish Medicines Agency

Lægemiddelstyrelsen should approve all testing of non-CE registered equipment. See http://www.laegemiddelstyrelsen.dk

Other authorities with control responsibility include Videnskabsetisk Komité (county level) and Ombudsmanden (national level)

The Danish Healthcare Data Network

The Danish SmartCare solution runs on the Danish Healthcare Data Network (DHDN) that gives the health sector in Denmark the possibility of offering their services to all the connected organisations through one secure digital connection. This is a part of protecting the patient's privacy and the data exchange. http://www.medcom.dk/dwn5350

Encryption and Decryption

All person-identifiable healthcare information transferred via external networks should be encrypted using the Danish Health Care Network.

The strength of the encryption keys shall be in accordance with the recommendations of "Persondataloven". The current minimum requirement for symmetric encryption is equivalent to 128 bits DES.

Healthcare Data Consideration

In compliance with Directive 95/46 EC, healthcare information is considered sensitive information. Sharing of patient information among healthcare personnel is only allowed based on consent from the patient.

Keeping of patient records is a legal obligation for the healthcare sector according to "IT-sikkerhedsvejledning for sygehuse", and is not based on informed consent.

Document Mandatory requirements

The security policy shall be available and documented in writing in accordance with "Persondataloven". A security examination of the IT systems of all healthcare organisations is conducted regularly by external accountants or auditors.

Overview of the national laws on electronic health records (Aportación OA, mantener?)

2.1.2.2 Spain

The following laws, royal decrees and resolutions from the Spanish government are the ones related to security to the provision of eHealth services:

1. The General Health Act (Law14/1986).
   The Act refers to the general regulation of all the actions that implement the right to healthcare as provided in article 43 and concordant provisions of the Constitution.

2. Law 16/2003 on the quality and cohesion of the National Health System.
   It establishes the legislative framework and consolidating legislation applicable to the National Health System to unequivocally identify users and patients (Health Card), the exchange of health information between the corresponding bodies, centres and services, electronic prescriptions and the communications network (Healthcare Intranet of the National Health System).

3. Law 41/2002 of 14 November, which provides the basic regulations for patient autonomy and rights and obligations regarding clinical documents and information.
   The purpose of the law is to regulate the rights and obligations of patients, users and professionals, as well as those of public and private health centres and services regarding patient autonomy and clinical documents and information.

4. Law 29/2006 of 26 July on guarantees and the rational use of health products and medicines.
Among other issues, the Law regulates medicines for human consumption and healthcare products, their clinical investigation, evaluation, authorization, registration, manufacture, preparation, quality assurance, storage, distribution, circulation, traceability, marketing, information and advertising, importation and exportation, prescription and dispensation, the monitoring of their benefit-risk ratio and the structuring of their rational use and the procedure for financing with public funds, where applicable.

5. Royal Decree 183/2004 of 30 January, which regulates the individual health card.
This Royal Decree regulates the issue and validity of the individual health card, the common basic data it is to include as standard, the personal ID code of the National Health System and the protected population database of said system.

6. Royal Decree 1093/2010 of 3 September, which adopts the minimum dataset for clinical reports in the National Health System.
The purpose of the Royal Decree is to establish the minimum dataset to be contained in clinical documents, regardless of whether they are created in electronic or paper format.

7. Royal Decree 1718/2010 of 17 December on medical prescriptions and dispensation orders.
It provides a new legal framework for medical prescriptions and dispensation orders that focuses on improving the rational use of medicines on a public and private scale and which, by helping to simplify work for health professionals, increases guarantees for citizens.

8. Legislative Royal Decree 9/2011 of 19 August on measures for improving the quality and cohesion of the national health system, contributing to fiscal consolidation and increasing the maximum amount for State guarantees for 2011.
It deals with measures related to the health information system and focuses on completing current processes for coordinating all health authorities regarding the health card, digital medical records and electronic prescriptions.

9. Royal Decree 81/2014 of 7 February, which provides rules for guaranteeing cross-border healthcare and amends Royal Decree 1718/2010 of 17 December on medical prescriptions and dispensation orders.
The purpose of this Royal Decree is to provide rules for enabling access to safe, high-quality cross-border healthcare and to foster cooperation in healthcare matters between Spain and the other Member States of the European Union.

Related information of the laws applicable can be also found at the Report contracted by the EC “Overview of the national laws on electronic health records in the EU Member States - National Report for Spain” [Ref. 1].

2.1.3 Regional Level

2.1.3.1 Scotland

NHS Scotland adopted one of the key recommendations from the Caldicott Report to establish Caldicott Guardians in each Health Board. (http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx)

The role of the Caldicott Guardian includes:

- a management audit of current practice and procedures;
- annual plans for improvement, monitored through the clinical governance framework; and
- development of protocols to govern the disclosure of patient information to other organisations.

These individuals oversee a range of information governance and assurance activities across the Board and are supported by staff at all levels.

The Caldicott principles cover:

- Data collection;
- Data usage; and
- Data retention.

Data usage includes access by clinicians, secondary uses and research access. Each organisation that wishes to access to the data held by NHS must have agreement from the relevant stakeholders and the Caldicott Guardian sign off to provide this access.

In addition to this, there are national and local information sharing agreements that are brokered and agreed between NHS, clinical communities and Local Authorities. These agreements must fit within the Caldicott principles outlined above.

Staff members are required to access certain data based upon the role they are asked to fulfil. This is approved by their management, and sets the users profile within the RBAC model. This means that when a clinician access the Clinical Portal, they can only see the data that there profile will allow them to. For non-clinical staff, they will not be able to see any data, unless they have been authorised to.

When a user logs into the NHS network, they are authenticated, and assigned an RBAC profile based upon the role they have been assigned. The profile will be used by the Clinical Portal to determine what (if any) patient data they can view. If they wish to update the patient record, then they must enter the underlying system, and may be prompted to log in to that system, otherwise the user profile they have from the initial login will still apply.

NHS policy is to ensure that IT systems can support the Caldicott framework, and staff in adhering to the code of conduct they sign.

A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see - http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText

2.1.3.2 Southern Denmark

The Shared Care Portal in the Region of Southern Denmark, which is a public entity, has been registered with the Danish Data Protection Agency as it contains personal data about citizens and as such is required by law to uphold the regulations stipulated in the Act on Processing of Personal Data.

When the tender for a regional PHR was published it was an invariable demand that the system live up to Danish law and regulations.

2.1.3.3 Catalonia

N.B.: All the aforementioned rules refer to the protection of health and the resources available in each autonomous community, as well as the organization of the powers that have been conveyed and the collaboration agreements between each autonomous community and the public corporation red.es.

The following laws, decrees and orders from the Government of Catalonia are the ones applicable to security on the provision of eHealth services:

1. Collaboration agreement by and between the public corporation red.es and Generalitat de Cataluña for the development of online healthcare (e-Health) as part of the Avanza Plan.

2.2 Security regulation on mobile devices, applications and services

2.2.1 Scotland

Tablet devices (Windows 8) will be provided to the actors as appropriate to their role within NHS GG&C. For certain clinical engagement, the use of tablet devices will not be appropriate to the clinical setting, and a desk based machine will be provided. This will also support the Clinical Portal. For remote access, the tablet devices will be provided with wireless connectivity, where available, and 3G minimum connectivity.

Wherever possible patient identifiable data will not be stored on mobile devices provided by NHS GG&C. Access to the clinical portal from remote devices will be through a live connection to the portal.

If data entry is required, and remote access is unavailable to an application, then the data stored on the tablet will be encrypted. this will be stored until the connection is resumed, and the data uploaded. On completion, the data is removed from the device.

In addition to the above, the tablet has a complex password implemented.

At present there is no PHR in the NHS. A national strategy is being developed, and NHS GG&C will be involved in the development of that strategy. A commitment has been given that the use of the Scottish Government 'My Account' will be the method by which citizens will identify and authenticate themselves prior to access NHS Scotland records. For further details on 'My Account' please see - http://www.scotland.gov.uk/Topics/Economy/digital/digitalservices/Sign-intoOnlineServices/myaccountBlogText

In terms of requirements for and any third party service or application to be integrated with the Health IT systems of the region and regulation related to the usage of mobile devices for healthcare related purposes, these must work in line with Data Protection Guidance in Scotland. There are a number of guidelines applied in Scotland where personal data is involved and these must be applied to acceptable levels.

A list of these can be found below, and the documentation is available on the e-health website:

http://www.ehealth.scot.nhs.uk/information-governance/

- Managing Information Assurance for mobile wireless services in NHSScotland: Good Practice Guide
- HARNESSING ONLINE SOCIAL NETWORKING WITHIN NHSSCOTLAND: BENEFITS AND RISKS
- EMPLOYEE AUTHENTICATION MANAGEMENT AND SINGLE SIGN ON: RISK ASSESSMENT AND GOOD PRACTICE GUIDE FOR NHSSCOTLAND
- EXTENSION OF EMERGENCY CARE SUMMARY (ECS) ACCESS TO SCHEDULED CARE SETTINGS IN SUPPORT OF MEDICINES RECONCILLIATION
- INTRA NHS INFORMATION SHARING ACCORD
- HANDLING REQUESTS FOR ACCESS TO PERSONAL HEALTH DATA
- ACCESSING PERSONAL INFORMATION ON PATIENTS AND STAFF: A FRAMEWORK FOR NHSSCOTLAND
- INFORMATION ASSURANCE ADVICE TO NHS BOARDS
- REVISED RECORDS MANAGEMENT: NHS CODE OF PRACTICE v2.1
  The Scottish Government has published a revised Records Management: NHS Code of Practice. The code is intended to be a guide to the required standards of records management practice for staff who work within, or under contract, to NHS organisations in Scotland. To accompany the Code, we have published nine operational Guidance Notes which provide practical guidance for those working at operational level within the Boards.
- CALDICOTT GUARDIAN WEBSITE AND MANUAL
  The Caldicott Guardian revised manual takes account of developments in information management in NHSS which have added to the Caldicott role since the publication of the first manual in 1999.
  In addition, a bespoke website for Caldicott Guardians is available at http://www.knowledge.scot.nhs.uk/caldicottguardians.aspx . The website supports the manual and should be seen as a "one stop shop" where topics are described in more detail with accompanying links to legislation, guidance and exemplar policies for use locally.
- INFORMATION GOVERNANCE CIRCULARS The following document contains useful links to a number of Scottish Government Health Department circulars relating to Information Governance. Infomation Governance circulars (Jan 11)
- NHS CODE OF PRACTICE ON PROTECTING PATIENT CONFIDENTIALITY
  This Code of Practice provides guidance to NHS employees on the necessary safeguards to maintain patient confidentiality. NHS Scotland staff are contractually obliged to adhere to the Code. It is available in pdf format below.NHS Code of Practice on Protecting Patient Confidentiality
- THE INFORMATION COMMISSIONERS OFFICE The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. All public organisations such as NHS Boards are legally obliged to protect any personal information they hold. The ICO has published a range of tools and resources e.g. Privacy Impact Assessments to help organisations understand these obligations and keep them updated as and when they change. Web link to main site: www.ico.gov.uk Link to the pages re Privacy Impact Assessments (PIA): www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

- NATIONAL ACCESS PROTOCOL APPROVED
- The eHealth Programme Board has approved a revised Access Protocol and guidance note for use on all NHSScotland eHealth initiatives. The protocol is to be used on current and proposed national eHealth systems and can also be used by NHS Boards for local level initiatives should they wish.
- The Protocol and guidance notes are in Word format below.Access Protocol template (March 10)Access Protocol Guidance Note (March 10)

2.2.2 Catalonia

TicSalut is developing a repository of health care apps that will be accessible by the Catalonia Electronic Health Record system (HC3) users through LMS (http://lamevasalut.gencat.cat)
Before publication, the apps will follow a strict accreditation process to ensure they comply with data protection and medical devices laws.

Health care professionals (HCP) can then advise the patient to use such applications.
The data collected and processed by such applications are incorporated to a secondary data base. HCP may then access the information provided by the apps and will be able to validate the data, to be incorporated into the patient's electronic medical record or to dismiss the information if it's incorrect or conflicting.

The apps will be reviewed periodically using the validations provided by HCP

3 References

Ref. 1 Overview of the national laws on electronic health records in the EU Member States - National Report for Spain, available at http://ec.europa.eu/health/ehealth/docs/laws_spain_en.pdf