# Talgildur samleiki

## Undirskjal 7 – Mobil ID

APRIL 2016

TALGILDU
FØROYAR
01100110 01101111

## Mobile ID

As the world around us gets more digital, the need for at digital identity grows. When we think of a digital identity there are various things we have a need to do. For example, we have a need to

- identify with a digital system
- sign documents in a non-reputable way
- communicate safely and confidentially

This is of course technically challenging. But it is also an organizational challenge to certify the validity of the registered identities. For that, we need policies and procedures.

In the countries around us we have seen that digital identity using mobile phone, is more and more common. And the advantages of mobile id are apparent.

- Most people on the Faroe Islands have their own mobile phone.
- Mobile phones are mainly personal, and we can use them for personal Mobile IDs.
- It is relatively easy to deploy, because the infrastructure is already in place.

It is therefore advisable for us to choose a digital identity based on mobile phones.

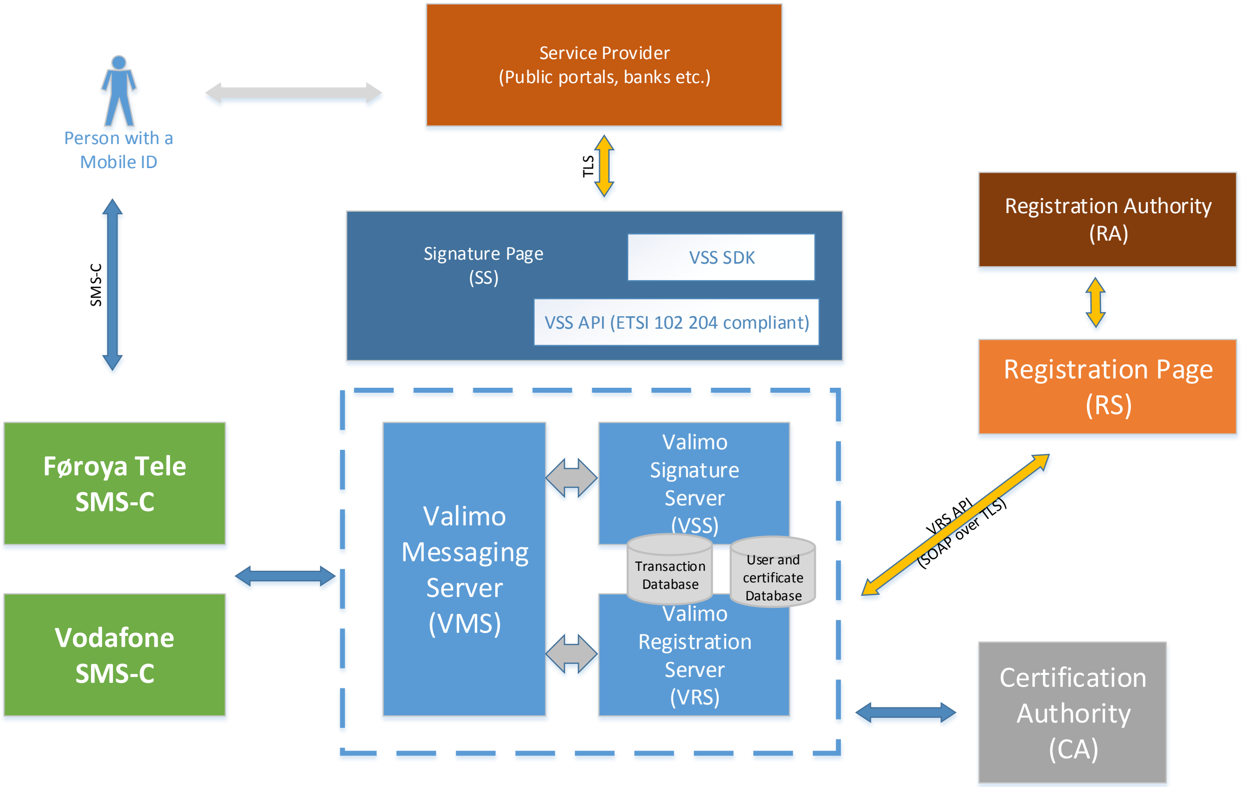
In the EU a need for a standardised digital mobile id has been identified. Countries like Iceland and Norway have shown interest in joining this standard, and we obviously should do the same. It is therefore a requirement for us to have a solution, that complies with [ETSI TS 102 204 V1.1.4] and the related specifications.

We have investigated suppliers fulfilling these requirements, and our recommended choice is to implement a solution from Finnish provider Valimo – a part of global provider Gemalto. This solution has been tested on the Faroe Islands as a proof of concept, and we think that it adequately satisfies our requirements.

We should keep in mind though that we in the future probably will have a need to exchange parts of our digital identity with something else. Including Mobile ID from Valimo. It is therefore important for us to find a solution that allows us to exchange the Mobile ID from Valimo with something else, without every service provider having to change their system's authentication as a consequence of this.

### Architecture

The figure below gives us an overview of the workings of the Mobile ID from Valimo and how it relates to the proposed solution.

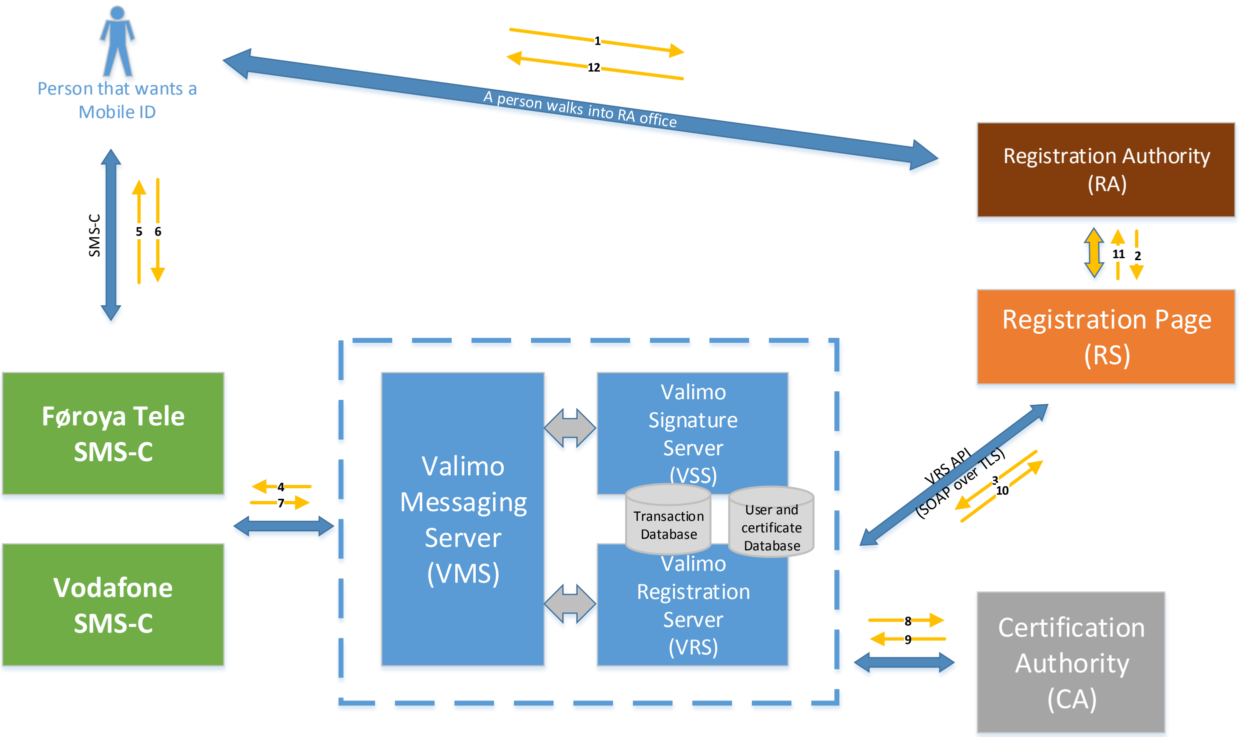


In the figure, we see the core components from Valimo as the blue components inside the stipulated box. Around all of this, we see the rest of the system as a collection of components that will mainly be developed by Faroese providers. Here we have the mobile network operators (MNO), a certificate authority (CA), a system for identity registration (RS) and a signature system handling login and sign requests (SS). Furthermore, we have a service provider (SP) corresponding to all the systems that will make use of our common digital identity and a registration authority (RA) responsible for the physical identification of persons and registration of this in the identity system.

The core solution from Valimo has 3 main components. The messaging server (VMS) communicating with the mobile network, the registration server (VRS) for managing Mobile ID registration process with the RA and CA for end user certificate issuance and  the signature server (VSS) to handle life cycle of mobile authentication and signing requests. In addition, we have various internal and external component that are required for the system to function correctly. We need

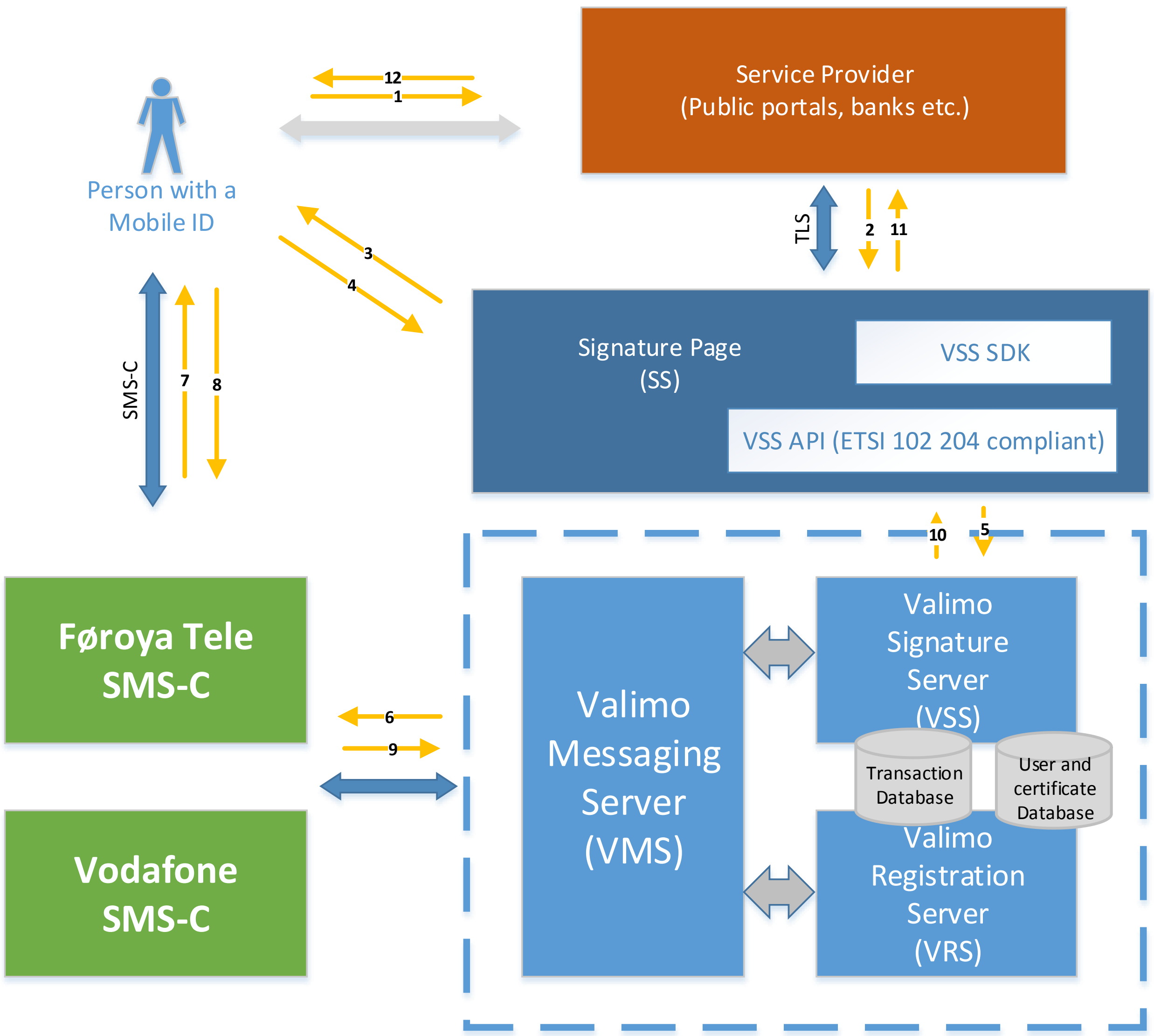
- to connect the Valimo core to the mobile network,
- a CA server,
- a connection to the mobile providers’ customer database and SIM provisioning system,
- to connect to the public ID registration system (FOLK) for personal validation purposes,
- to save all issued certificates internally in the Mobile ID database for signature verification and
- to log all transactions in a transaction database.

The diagram below demonstrates how a normal registration event would look like.


Person that wants a Mobile ID
1
12
A person walks into RA office
SMS-C
5
6
Registration Authority (RA)
11
2
Registration Page (RS)
Føroya Tele SMS-C
Vodafone SMS-C
4
7
Valimo Messaging Server (VMS)
Valimo Signature Server (VSS)
Transaction Database
User and certificate Database
Valimo Registration Server (VRS)
VRS API (SOAP over TLS)
3
10
8
9
Certification Authority (CA)

1. It starts with a person that walks into a registration office to get his Mobile ID.
2. The Registration Office personnel make necessary background checks and then fill out the required information in the Registration System.
3. The Registration System calls a SOAP API on the VRS to start the Mobile registration process; the VRS constructs the necessary commands which are sent to the SIM card applet.
4. The VMS server forwards the registration request message through MNO SMS-C to the person’s mobile phone and the Mobile ID SIM applet.
5. The person receives the registration request in an encrypted binary SMS, which triggers the Mobile ID applet requesting the applet to create private and public keys as well as asking the person to select a password (PIN code) to protect the private key.
6. When the key pair has been generated and user has chosen the PIN code, the Mobile ID applet sends a certificate request (PKCS#10) back to the VRS.
7. The MNO SMS-C relays the response to the VRS through the VMS.
8. The VRS sends the certificate request to the Certification Authority (CA).
9. The CA returns a valid and signed certificate that is stored for reference in the Mobile ID database.
10. The VRS then returns response to the registration request to the registration system.
11. The registration system displays a success message on the screen.
12. The person is told, that his Mobile ID is now active. Alternatively or in addition, the person will receive an SMS informing the success of Mobile ID registration.

Below we see an example of a Mobile ID authentication.



1. A person with a Mobile ID enters the service provider's (SP) home/login page and clicks on a login link.
2. The SP hands over control of communication to the signature page (SS).
3. The SS presents the user with a choice of login methods and follows with a sign in screen for Mobile ID.
4. The person enters his mobile number.
5. The Signature Page (SS) calls the VSS API with a sign request to authenticate the user.
6. The VSS constructs the commands for the request and asks the VMS to send the signing request to the user’s phone.
7. The VMS sends a binary SMS containing the signing request to the user’s phone and Mobile ID applet through the MNO SMS-C.
8. The binary SMS triggers the Mobile ID applet; user reads the request and enters his PIN to unlock the private key to sign the data in the request and then to return the response message.
9. The message is returned back to the VSS by the MNO SMS-C through the VMS.

10. The VSS checks the signed message data verifying the signature and validating the status of the person's certificate (i.e. certificate not expired or revoked) and returns back to the SS the response to the signing request with status of the signature (Ok, not OK).
11. The SS returns control of communication with the user to the SP.
12. The user is presented with a successful authentication. and possibly also the signed data e.g. signed hash of a document

## The security of Mobile ID

Mobile ID is based on a PKI infrastructure and we know it is used in technologies like TLS and SSL. In fact, Mobile ID is based on exactly the same certificates that TLS and SSL use called X.509 certificates. And as with those certificates, a core part of the security in it is about how the holder of the certificate is authenticated, and how we can make sure the private key corresponding to the certificate is kept safe.

### *Creation of certificates*

When we create certificates for users of Mobile ID, there are two different basic pillars, that together make up the validity of the certificate and the private key. One is about processes and policies which will be covered elsewhere, and the other is about technical protocols. For the technical part, a general overview of how SSL certificates are created is explained here: [http://www.zytrax.com/tech/survival/ssl.html#trust]. Mobile ID follows this process, but in a way, that also connects the certificate to the private key stored inside the SIM card on the mobile phone. In [Valimo Mobile ID - User registration and transaction flows and sequences[0.1].pdf] slide 4 we see how certificates are created and the private keys are kept safe in the Mobile ID solution. It is worth to note that only the public key is returned together with the ICCID in the certificate request. The private key is securely stored on the SIM card. As an extra security measure, the use of the private key is controlled with a PIN on the SIM-card. This ensures, that only the person knowing the PIN, is able to use the private key.

The SIM card chip itself can be considered a “mini computer” that can do its own cryptographic operations. Hence, the private key does not need to, and never will leave the SIM card chip.

Regarding the created certificate, we do not have any concerns about distributing it, because it will only contain the public key along with a mapping to the ICCID. The CA validates the mapping through the created certificate.

### *Signing with Mobile ID*

In [Valimo Mobile ID - User registration and transaction flows and sequences[0.1].pdf] slide 6, it is explained what happens, when a user signs using Mobile ID. Authentication is a special case of signing, so the process of authentication using Mobile ID is the same. In the flow it is worth to consider step 5, where the request is pushed to the SIM card for signing. What happens in this step is that

a) The mobile phone receives a signing request with an encrypted binary SMS from Mobile ID core (VSS).
b) The content of the SMS is processed on the SIM card, and the phone user is prompted to enter his PIN for the private key.
c) When the private key is unlocked, it is used to sign the request.
d) And finally the signed request is sent back through the SMS channel.

When we have an authentication request, the signed data is an authentication token, and when we get a request to sign data, the signing request contains text or a hash of the data the user needs to sign. This last part can be difficult for the user to understand, and we need to make sure the user understands this.

## Explaining the components

### *Valimo Registration Server (VRS)*

When a person wants a Mobile ID, this needs to be registered through an API to the VRS component. This API is an SOAP API, that is relatively simple to use. It contains operations on 3 different kinds of entities: Person ID, SIM cards and Certificates, and their relations. See [Valimo_VMS_Product_Overview] for a high level explanation of VRS and [Valimo_VRS_API_Description] for a more detailed description of the API operations and calls.

### *Registration Authority (RA)*

We need to choose who is going to register users of the Mobile ID on the Faroe Islands. The RA is the institution or office that has the mandate to register a Mobile ID as the digital identity of a person. The RA will have access to a registration system, where required functionality of the VRS API is called. This system will also be connected to other systems relevant for the establishment of the identity.

## Registration system (RS)

The registration system will be a web application, where the RA will register the users of a Mobile ID. This page will also handle registration of other kinds of digital IDs like the Card ID. It is important that this system is flexible, such that we in the future will be able to change or add to the list of digital signatures.

This system will probably also need to handle usage from users with different authorization level. We could for example imagine an RA certifying users at the highest level, bank personnel only certifying a person at the second level and finally a company administrator giving his employee access to a company ID.

### *Certificate Authority (CA)*

Mobile ID requires a CA server to function. A detailed description of what a CA is, is provided elsewhere in the report, and we will not delve deeper into this. But the short technical explanation is that a CA is a service that contains a trusted root certificate, which issues and validates certificates for the digital identities.

### *Valimo Signature Server (VSS)*

The signature server is the core component, that is most exposed to the outside. The signature server is, among other things, able to

- Request user to authenticate with a Mobile ID
- Request user to sign a document with Mobile ID

Every Service Provider that wants to use Mobile ID, will have to register with the VSS, before it can start using the Mobile ID for Digital ID operations.

#### VSS API

Communication with VSS is done through a SOAP API that complies with the ETSI TS 102 204 standard [ETSI TS 102 204 V1.1.4]. An example of how to use the API can be seen in the document [Valimo Mobile ID - VSS

SOAP call examples]. It is important that communication with the API is done through a TLS encrypted connection.

#### Valimo VSS SDK

Valimo does also provide an SDK for coding against VSS in Java. The SDK uses the VSS API internally and handles some of the complex details of calling the API correctly. We recommend that a sample implementation should be done to find out, how complex it is to use the API directly instead of using the SDK. A detailed description of the VSS SDK is given in the document [Valimo_MSS_SDK_Guide].

### *Transaction Database*

Any action taken on the Valimo APIs is logged to a transaction database. This is an important feature, because we don't want the user of a Mobile ID to be able to repudiate his actions. The transaction log does also enable us to query information on the usage of the signature system. We could for example have a page showing all the usage of my Mobile signature.

### *Service Provider (SP)*

A Service Provider is any system that enables its users to authenticate or do signing actions with their digital ID, including Mobile ID. Examples of services that a SP provides are

- Logging into internet banking
- Signing application for child care
- Signing application for elderly care
- Digital communication with the social agencies
- Digital TAX reports
- Property ownership registration (Tinglýsing)
- Sending applications for ALS (unemployment agency)

The Mobile ID solution from Valimo has different possibilities for accessing the signature capabilities as explained above. But it is important to keep in mind that we do not want to lock into a specific digital ID vendor or solution. We need to supply a second digital ID in the Card ID, and we might have to supply other solutions very soon. To mitigate this risk, the SP should not be connected directly to the Valimo VSS API, but instead connect through a special purpose API, shielding the SP from implementation details and future changes in providers.

## Signature Page (Samleikasíðan or SS)

The plan is to provide this screening with a component that we call the Signature Page (SS). The idea is that the SP links to the Signature Page for login functionality, and lets the Signature Page handle the user authentication. When ready, the Signature Page leaves control back to the original system, and the user will be able to start his usage as the authenticated user.

The idea is also to let the signature page be responsible for following security best practises and other cross cutting concerns like logging or certificate validity checks.

It is worth to consider if we should implement the Signature Page in conformance with globally acknowledged standards like OpenID Connect over OAuth 2.0 [see http://openid.net/connect/] or other alternatives.

*Valimo Messaging Server (VMS)*
The messaging server is the component responsible for the communication with the mobile phone through the mobile network. This communication has to be highly secure and at the same time it is fairly standardized. It will therefore be implemented by Valimo. For security reason we do not have detailed information about how the communication is implemented, but Valimo has stated, that it is following the [GSM 03.48] standard for encrypting the SIM applet messages end to end. An overview of how this is implemented can be seen in the documents [Valimo_VMS_Product_Overview], [Valimo_VMS_Administrator_Guide] and [Valimo_VMS_Installation_and_Configuration_Guide].

*The mobile network*
It is a prerequisite for Mobile ID, that digital authentication and signing is done through the mobile network. The implication is that the core of Mobile ID has to be connected to the mobile network on the Faroe Islands. Each phone that is to be used as a Mobile ID, will be equipped with a specially produced SIM card, where it is possible to put the private key of the Mobile ID.

A proof of concept implementation of the Valimo Mobile ID has been tried on the Faroe Islands, so the required implementation of the connection between the VMS and the two operators has already been implemented.

*ICCID card database*
Information on the SIM cards and their holders is usually saved in a customer relation database of the MNO. It is unclear at the moment if we should have a central registration, or if we should let the mobile operators keep these records for us. But in any case, the Valimo system needs to be integrated with our choice of registration system which in return needs to integrate with the CA. The RA/RS will need to store information about the registered users.

### Integration points

Valimo has provided a document showing the interfaces that will be specially developed for our solution [see Mobile ID PKI Integration Points 10032016]. The document is both identifying each interface to be developed, but also assigns responsibility to all the common tasks in the implementation process. It is therefore a valuable tool in our implementations process.

### Mobile APP from Valimo/Gemalto

Valimo/Gemalto is in the process of developing a Smart Phone App for use as a Mobile ID. The App is planned to be rolled out in production during the summer and fall of 2016. Allowing the mobile ID to be implemented through an App instead of running with SIM card security, has various advantages and disadvantages. An overview of the product can be found in the document [Gemalto Mobile ID for Smartphone_4.2.2016].

Some of the advantages are:

- App security does only require internet and hence not a Faroese phone operator.
- A Mobile App does not require special hardware to function. I.e. no card reader.
- A Mobile App enables fingerprint authentication if the phone supports it.
- Other kinds of biometrics could be developed if secure enough.

Of the disadvantages we could mention that

- The security is lower than for the pure mobile network solution.
- The Mobile App is a new product and therefore not tested in production yet.

Valimo have presented various measures they have taken to improve the security. And even though it is less secure, we find that this solution might be secure enough to be implemented on the Faroe Islands. But concerns have been raised about the product not being tested in real life yet. The banks' IT solution provider has declined to be a frontrunner on any technology, and it is therefore important for us to wait and see how this solution works out.

Our conclusion is therefore that this is an interesting ID solution, which solves some of the concerns of the other solutions we consider. It is not as secure as the mobile network ID, but it might be secure enough. We should not launch it with our first version of a digital ID, but we should certainly plan for it to be introduced at a later stage.

### Other concerns

*Monitoring*
If Mobile ID is to be the core of the Faroese digital identity, it is important that it is operational at close to any time. We need to check if the system is running, and the right person needs to know when it does not. Furthermore, we need to see when the system is under pressure. The Valimo solution provides the possibility to expose the system health through various functionality like for example a Heart Beat function.

*Reporting*
We will have a need for usage information of different kinds. Valimo is able to provide us with this information through their transaction logging. Alternatively, we could log the same usage data in other parts of our system and handle the necessary reporting ourselves. Interesting information could be: general usage, number of users or perhaps what SP systems are used the most.

## Assessment of the mobile solution and how it fits with the overall solution

The Digital ID will service the country for many years to come, and it is important for us to make a thoroughly considered choice about what digital ID we implement. A lot of questions need to be answered and concerns have to be raised. We will try to do this, but first we will make an overall assessment.

The mobile solution from Valimo is generally well suited as a digital id for the Faroe Islands. The solution has already been tried out, and we have seen it working. The solution also fits well into the overall solution.

There have been concerns about the usability of the mobile compared to the currently deployed NemID solution at the banks. Mobile ID is limited as a solution for persons not living on the Faroe Islands. Hence, we need a different solution for these persons. Furthermore, it has been raised as a possible issue that SMS traffic sometimes gets none or low priority, and this might result in lost or seriously delayed messages. It has not been reported as an issue from other customers of Mobile ID from Valimo though, and we do not expect it to be a serious issue. This is not a concern as long as you are on the Faroese mobile network because we will be able to provide priority to the messages.

Another concern that has been raised is in regard to all the sailors living on the Faroe Islands. They are often situated far out on the sea, and mobile connection is through satellite. SIM based Mobile ID will probably not always function here.

The conclusion is therefore that the Mobile ID is a good solution for the Faroe Islands, but that it cannot be the only digital ID solution.

## What do we need to do?

Mobile network operators need to be connected to the Mobile ID solution from Valimo. This includes a distribution of new specially produced SIM cards and VMS integration at each MNO.

A Certificate Authority (CA) needs to be founded. It is preferred that this is delivered by a Faroese provider, but this can be a problem when we want our digital id approved internationally. If we want to run this on the Faroe Islands, it is important that we get the right guidance in the process and that we educate people with the right competences.

A registration authority must be founded to handle registration of digital identities for the citizens.

An administration system must be developed to enable the digital registration and administration of digital ids and corresponding certificates. Mobile ID should only be part of this system.

It is recommended that a common signature page should be developed, such that every service provider does not have to create and maintain its own. The purpose of this is also to shield the individual service providers from the specific signing mechanisms and to make it easier to make changes to the digital id in the future. This signature page should also provide a means to sign data digitally.

## Statements and recommendations

Mobile ID is tied to the Faroese mobile phone operators and this makes it impractical to provide Mobile ID to people not living on the Faroe Islands. We need another solution that can handle this.

In the future, digital identities will probably be used across borders. It is therefore recommended that we think this into our solution from the beginning. There are two requirements in this. To handle foreign identities in our systems, and to enable foreign systems to handle our signature in their system. As a first step, we should make sure our identities are properly confirmed such that they will be recognized internationally.

Some of the world leading IT companies in the world are working together on a sign in standard called Open ID. The latest version of this is Open ID Connect which is based on OAuth 2.0. It is our recommendation that we try this standard out, and if we find it suitable, implement it in our signing solution. The Open ID standard is mainly about authentication. So we might have to take different actions in regards to document signing.

Gemalto (Valimo) has a standard system that implements OpenID Connect, but it is not recommended to use it, because we would lock too tightly into a single ID provider.

We must make sure, that our solution meets the needs in regards to monitoring and reporting. We need to monitor the status, stability and general health of the system, and we also need possibilities to query the usage of the system in various ways. Valimo is probably able to provide us with most of this, but we can also consider to develop some things on our own.