DATA PROTECTION IMPACT ASSESSMENT

REPORT

Name of process/ information system / program:	**IRMA project**
Name and contact details of data controller	**Privacy by Design Foundation** info@privacybydesign.foundation Toernooiveld 212, 6525 EC Nijmegen, The Netherlands Website: https://privacybydesign.foundation/en/
Name and contact details of the people involved in the DPIA:	Authors: LLM Katerina Demetzou, PhD Candidate at Radboud University K.Demetzou@cs.ru.nl LLM Tim Walree, PhD Candidate at Radboud University t.walree@cs.ru.nl

	Reviewer: Dr. Koen Versmissen, FIP Partner at Privacy Management Partners, Vondellaan 46, 3521 GH Utrecht koen.versmissen@pmpartners.nl *This Report has been written by Katerina Demetzou and Tim Walree, in an independent role, in order to build up practical experience with privacy impact assessments, as part of their PhD work. The Report has been reviewed critically by external expert Koen Vermissen.*
Date of DPIA report:	10/12/2018

Table of Contents

1. INTRODUCTION

Article 35 of the General Data Protection Regulation (hereafter, GDPR) requires that data controllers perform a DPIA (Data Protection Impact Assessment) in cases where processing of personal data is "likely *to result in high risks to the rights and freedoms of natural persons*". This is a legal obligation for data controllers. When it comes to software developers (as is the case for the Privacy

by Design Foundation, hereafter, the Foundation), such an obligation is not legally imposed. It is recommended however as a best practice by the WP29[1]. Developers are encouraged to perform an impact assessment of the product/service they develop so that it substantially informs the data controller when performing their DPIA. Both Recital 78[2] as well as the privacy by design obligation of Article 25 point towards this direction.

In this line, the Foundation which is the developer of the IRMA app, has performed an impact assessment for this specific product. With regard to the scope of this Report, one clarification should be made. The Foundation is the developer of IRMA. But it is also a data controller given that it processes personal data (as will be explained in more detail below). However, as a data controller the Foundation processes only a minimum of personal data of the users, and does not fall under any of the categories[3] whereby the legislator requires the performance of a DPIA. Therefore, this Report, while talking about the Foundation's role as a data controller, will mainly focus on the product itself, its description and the way in which it is developed in order to safeguard the privacy and data protection of the users.

One further clarification to be made is that at the time this Report is being developed the Foundation is the main Issuer of attributes. However, this is not the envisaged model of IRMA and this is the reason why we refer to it throughout the Report as the 'current model'. Once, more Issuers get involved in the IRMA ecosystem, then the way in which they will handle their interactions with the users will be their responsibility, given that the Foundation is not directly involved in the attribute issuance sessions: attributes are issued directly to the user and do not pass though the Foundation.

Documents consulted for this Report:

- ISO/IEC 29134 "Information technology – Security techniques – Guidelines for privacy impact assessment",
- WP29 Guidelines on DPIA 248 rev.01,
- ENISA, Guidelines for SMEs on the security of personal data processing.
- CNIL, Methodology for Privacy Risk Management, 2012

Planning for DPIA update: This Report will be updated in light of significant changes and, in any case, at least every two years.

[1] WP29 Opinion on DPIA

[2] Recital 78 GDPR: *"[…] producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations."*

[3] Article 35 GDPR, guidelines from the WP29 with the 9 criteria

2. SYSTEM DESCRIPTION

2a. Textual description

Nature of the processing:

IRMA (stands for *I Reveal My Attributes*) is a collection of software applications designed and developed by the Foundation. This software has been developed for the purpose of privacy-friendly authentication and for the purpose of attribute-based signing in the online environment. It is an example of *privacy by design*, given that privacy is an intrinsic consideration and element of the system. It is an example of attribute-based identity management.

Purpose of the processing:

The purpose of IRMA is to provide to its users a privacy friendly way to authenticate themselves and to sign online when making purchases or when using services. It empowers the user to disclose online, via the mobile phone, certain attributes (eg. “over 18”) but at the same time to hide other attributes.

Scope of processing:

The scope of the processing is limited to the purpose of IRMA. Upon registration, the Foundation collects and stores only the blinded PIN code, and optionally the email address of the user. Given that for the time being the Foundation is a main Issuer of attributes, it also processes (collects and stores) user information in order to provide the user with the requested attribute(s). This information is immediately deleted once the attributes have been given to the user. In the future and as more organizations join IRMA, the Foundation will keep its role as an Issuer, but in fewer cases.

Context of processing:

IRMA is based on non-trivial cryptography for attribute-based credentials. These credentials are containers for attributes, equipped with an expiry date and a digital signature, produced by the Issuer. The underlying cryptography is based on Idemix, which has been developed since the late nineties at IBM Zürich. The technology is open and has been published in the scientific literature. This contributes to confidence. The Foundation has developed its own, different, independent, open source IRMA implementation of Idemix.

2b. Visual flow chart

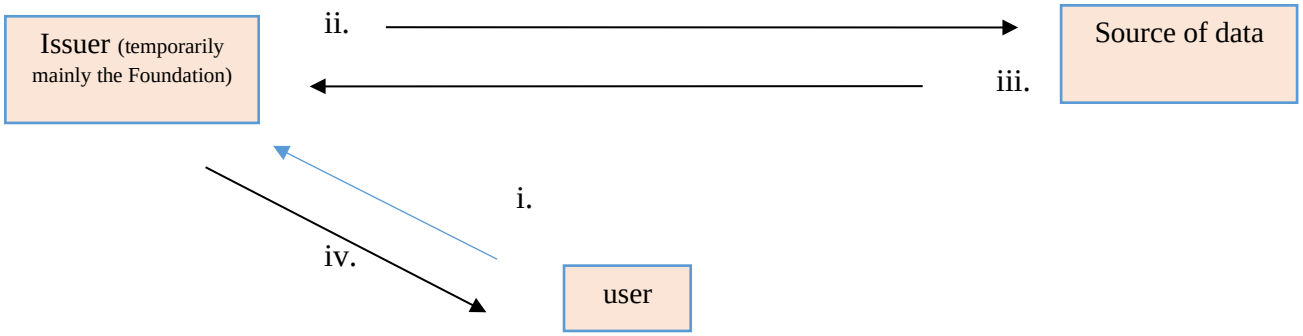
1st type of processing operations:

Email address, blinded PIN code

Purpose of processing:

- registration of the user with IRMA
- IRMA functionality

2nd type of processing operations:



i.: the user requests the Issuer for attributes,

ii.[4] : the Issuer requests from the "source of data" information that is necessary for the specific credential type,

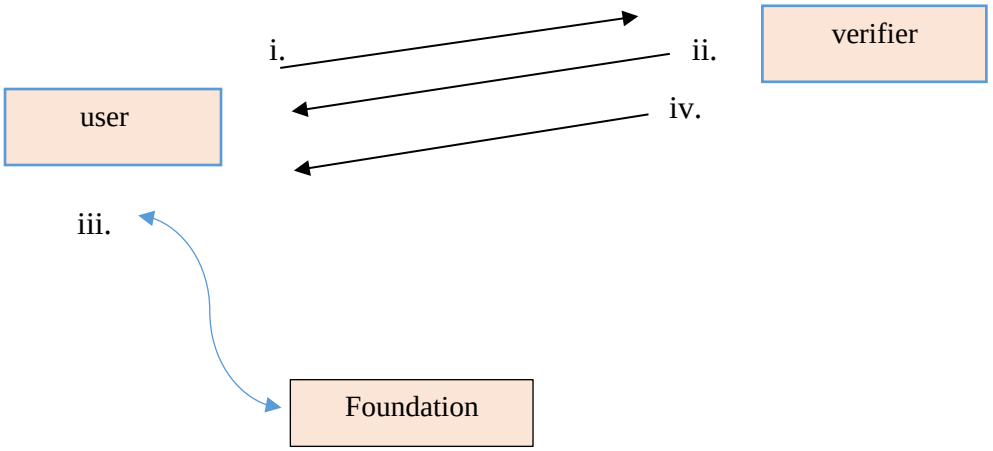
iii.: the "source of data" provides user data to the Issuer through a protocol,

iv.: The Issuer provides the user with the requested credential, that is stored locally on the user's device.

Purpose of processing: to provide the user with the requested attribute(s)

[4] It is not always the case that relevant information is requested from the "source of data". For example, for the email address attribute (https://privacybydesign.foundation/issuance/email) the email address (which is the data) is entered by the user herself.

3rd type of processing operations:



i.: the user asks for a service,

ii.: the verifier asks the user to reveal the relevant attribute(s) in order to provide the service,

iii.: The user enters her PIN code, blinds it, and sends the blinded version to the Foundation, which checks it. If it is correct, then the Foundation contributes to the user's attribute disclosure (this contribution is required for the user to be able to proceed with the disclosure).

iv.: the user discloses the requested attribute(s) to the Verifier and the Verifier authenticates the revealed attribute(s) and provides the service to the user.

Purpose of processing: user authentication (and disclosure of attribute(s)) and signing online.

4th type of processing operations:

The user wants to deregister from MyIRMA.

The Foundation deletes all data of this user from the MyIRMA server.

Purpose of processing: Deregistration of the user.

3. QUESTIONNAIRE

Nr.	Question	Answer	Addition
	Personal data		
	Is there processing of personal data by the Foundation? If yes, what are the types and their nature?	There is processing of personal data when the user registers at IRMA. More specifically: ✓ **Blinded PIN code**: A PIN code is required when the user registers with IRMA for the first time. Every time a user authenticates with IRMA, by revealing IRMA attributes, this PIN code is required. Digital signatures also require it. The Foundation does not store the PIN directly; instead the PIN is blinded before it is sent to the Foundation by a random piece of data	

		that never leaves the phone. This ensures that (1) the Foundation does not know the user's PIN, and it is not possible for it to learn the PIN through e.g. brute forcing; and (2) that when two users happen to use the same PIN, that this is not visible to the Foundation. ✓ **Email address** is optional when the user registers with IRMA for the first time. In case the user provides her email address it will be used to contact the user, if needed, about the usage of IRMA. This address will not be shared with others. The email address and the blinded PIN code are only <u>processed for the purpose of registration of the user and for contacting the user for reasons of security</u>. The processing operations for the purposes of downloading attributes from the Issuer and disclosing attributes to the Verifier, include only the processing of those attributes. <u>What is an attribute</u>? An attribute is a personal property. It forms a natural mechanism for revealing certain aspects of yourself, while at the same time selectively disclosing other aspects. It provides precisely the relevant information that is required for a certain transaction. Attributes are equipped with an	

		expiry date and a digital signature, produced by the Issuer. Examples of attributes: ▪ I'm a student (or a pensioner) ▪ I'm older than 12 (or 16, or 18, or 21, or 65) ▪ I'm younger than 12 (or …) ▪ My nationality is … ▪ My gender is … ▪ My bank account number is … ▪ My home address is … ▪ My given/family name is … ▪ My national registration number is … ▪ My insurance number is … ▪ My email address is … ▪ My mobile phone number is … ▪ My loyalty card of company X has status bronze / silver / gold ▪ My rail subscription is first / second class	

		There are two categories of attributes: attributes that are **uniquely identifying** (eg. Bank account number is associated only with one person) and attributes that are **not identifying** (eg. Gender). Combinations of non-identifying attributes may together still identify a user[5]. When an attribute is issued to the user that requested it, **it constitutes personal data** for a minimum period of time that is required for the attribute to be sent to the IRMA app. Usage data: The Foundation records usage data ("logs") per account. Its sole purpose is to provide to the IRMA user insight in the usage of her own account, associated with the user's email address, in order to detect possible abuse and to (subsequently) block the account. With this access to a user's own log data the Foundation fulfils its obligation to provide users insight in their own data. These log data are stored and protected until they are deleted by the user. The logs contain only time stamps of actions, together with the kind of action that happened, such as PIN verified or IRMA session performed. In particular, these logs do not contain personal data, such as attributes, or	

[5] See below, section 6.4

		information about the party to which attributes are revealed, or from which attributes are received. These log data are not shared with others, unless there is a legal obligation to do so. When an IRMA account is terminated, or when its data are removed, all these log data are immediately removed by the Foundation.	
	Does the Foundation store personal data? If yes, where is the personal data stored?	➢ Email address and blinded PIN code: With regard to the email address and the blinded PIN code of the user, they are both stored in a special server which is located in the Netherlands and is called "MyIRMA". This storage is for security reasons. What is important to highlight is that the user's PIN code cannot be deduced given that what is stored is a blinded version of the PIN code. ➢ Attributes when issued to the user: When the Foundation (temporarily the main Issuer) requests information from the "source of data", upon a user's request, it only stores the relevant information on its server, for the time needed to give the attribute to the user. After the attribute is provided to the user, it is immediately	

		deleted from the Foundation's server and is only stored locally (ie. on the user's device).[6] The Foundation does not store information with regard (1) to which Verifier the user has revealed attributes or (2) from which Issuer the user has received attributes. Were this not the case, the Foundation would become a giant privacy hotspot. Thus, when logging into MyIRMA the user cannot see this information. When the user decides to terminate IRMA on the MyIRMA webpage all data are immediately deleted. Thus, if the user wants to use IRMA in the future, she has to re-register from the start. IRMA uses a decentralized architecture: That means that the attributes are stored only locally, on the user's phone, and not centrally in the computer systems of some "identity broker".	
Controller			
	Who is the controller? E.g. who defines the 'means and purposes' of the processing?	The Foundation is a data controller with regard to the personal data it processes as explained above. Issuers, Verifiers and the "source of data" are also data controllers as to the personal data they process.	
Other actors involved			

[6] This is the case with all Issuers (not only for the Foundation as Issuer).

	What other actors are involved in the IRMA ecosystem?	**<u>The attribute Issuer</u>**: it is the organization that provides one with her attributes. The Issuer digitally signs[7] the attribute and also attaches an expiry date in a cryptographically secure way. It may be the case that the Issuer is different from the "source of data". Examples of possible Issuers: - national or local (government) authorities, for attributes like: name, address, date of birth, national citizen numbers, categories of income, etc. - banks and insurance companies, for attributes like: bank and/or insurance account numbers, type of insurance, etc. - internet service providers and telecom operators, for: email addresses, phone numbers, IP-addresses - the Facebook's / Google's / Apple's / Amazon's / Microsoft's of this world for login data - big or small web shops, with loyal cards and custom numbers, with associated status, coupons, etc. For the time being, the Foundation is the main Issuer. Upon user request, the Issuer requests from the "source of data" (when necessary) only the information that is necessary according to the	

[7] The digital signature is formed by a private key and a public key. This couple of keys is generated by the issuer. The issuer stores the private key and publishes the public key. The verifier uses the public key to verify that it indeed couples with the private key and thus origin and integrity of the attribute are guaranteed (this is called asymmetric signing).

		credential type. User data are sent to the Issuer through a protocol that ensures that only relevant information is disclosed. **<u>The Verifier / the relying party:</u>** It is the requesting party that asks for some attributes in order to authenticate the user and provide its services. - Attributes in IRMA carry a digital signature of the Issuer. Via this signature the Verifier can check the origin and the integrity of attributes. - When the user wants to prove for example to a web shop that she is older than 18, IRMA app communicates directly with the web shop, without intermediary parties. (intermediary parties which exist in centralized systems, can track the user's behavior and create profiles – which does not happen in a decentralized system)	
		Data subjects	
	Who are the data subjects?	Any natural person who registers with MyIRMA is a data subject.	
		Lawfulness – Legal Ground	
	What is the legal ground for processing?	<u>User's consent</u> constitutes the legal ground for all processing activities that take place. IRMA is entirely based on consent. The ground of a contract cannot apply in this case given that registration with MyIRMA does not form part of	

		any contract. It is a user's choice to register and use the app.	
	If based on consent, how is consent asked?	A user of IRMA is asked to consent (agree) at every data processing step by the IRMA app or the Foundation's website. A user can withdraw her consent at any stage and terminate the Foundation's processing of her personal data by terminating (blocking) her personal IRMA account, via the MyIRMA webpage. The IRMA app asks the user to consent whenever attributes are received or revealed, not only via an OK button but also via confirmation with a personal PIN code. This forms the legal basis for the processing of the relevant attributes by the actors that provide or receive attributes.	
Purpose(s) of processing			
	What are the purpose(s) of processing?	There are five main groups of processing operations that take place in order that IRMA achieves its overall purpose. More specifically: 1. Processing for the purpose of user registration. 2. Processing for security reasons 3. Processing for the purpose of providing the user with the requested attribute(s) 4. Processing for the purpose of authenticating the user and of signing online. 5. Processing for the purpose of deregistering from the app	

		(deletion of data retained by the Foundation)	
Data protection by design			
	In what way has data protection by design been taken into account?[8]	- **Decentralized architecture**: That means that attributes are stored only locally, on the user's phone, and not centrally in the computer systems of some "identity broker". - **Selective disclosure of attributes** that are contained in a credential (eg. A credential may contain attributes such as: nationality, place of birth, date of birth) - **Issuer unlinkability**: This means that an Issuer cannot trace the disclosures of these attributes by a user, not even when the Issuer colludes with a Verifier and both parties put their data together. Of course, this does not work for identifying attributes, like the bank account number, but it does work for non-identifying attributes, like "gender". - **Multi-show unlinkability**: when someone discloses the same non-identifying attribute (e.g. her gender attribute) twice, then it is not possible for the Verifier to link these two transactions	

[8] See below, Section 6 for a more detailed analysis of the privacy by design of the IRMA app.

		as coming from the same user. Put differently, this situation is indistinguishable for the Verifier from two distinct users both disclosing their own gender attributes (that happen to have the same value). This means that someone's attribute disclosures over time cannot be linked.	
Data minimization			
	Does the controller process only the data that are necessary for the purposes to be achieved?	Under the current model where the Foundation is the main Issuer, when the Foundation requests to the "source of data" the attributes that the user wishes to obtain, only the information that is relevant for the credential type is provided through a protocol. Upon disclosure of attribute(s) to the Verifier, only the attributes which are relevant and necessary for a transaction are disclosed.	
Data accuracy			
	How is the accuracy/integrity of the personal data safeguarded?[9]	Attributes in IRMA carry a digital signature of the Issuer. Via this signature the Verifier can check the origin and the integrity of attributes. Attributes have an expiry date, which can also be checked by the Verifier. If attributes have expired, they need to be refreshed by the user, by returning to the original Issuer.	
Data retention			

[9] See also below, Section 6.2

	For what period are personal data processed?	When the Foundation (temporarily the main Issuer) requests information from the "source of data", upon a user's request, it only stores the relevant information on its server, for the time needed to give the requested attribute(s) to the user. After the attribute(s) is provided to the user, it is immediately deleted from the Foundation's server and is only stored locally (ie. on the user's device). The Foundation does not store information on which Verifier the user has revealed attributes to or from which Issuer the user has received attributes. Thus, when logging into MyIRMA the user cannot see this information. When the user decides to terminate IRMA on the MyIRMA webpage all data are immediately deleted. Thus, if the user wants to use IRMA in the future, he has to re-register from the start.	
Transparency			
	How are data subjects informed of the processing?	The Foundation provides for a detailed description through its Privacy Policy as well as via "IRMA in detail". Further technical information on how the IRMA app works can be found on the Privacy by Design Foundation's website.	
Data subjects' rights			
	How are data subject rights respected?	All data subject rights that are enumerated in Sections 2, 3, 4 of the GDPR (ie. right of access, right to information, right to rectification etc) are respected. The user is the one who choses and	

		requests from the Issuer the precise attributes she wishes to download to her IRMA app. The user has genuine control over the usage of her own attributes: she directly discloses her own attributes herself, every time only after explicit consent, without (unnecessary) interference of third parties. The Foundation is in the process of developing policies and procedures to specifically illustrate how data subject rights can be enforced.	

4. RISK ASSESSMENT

Article 35 GDPR, requires that the high risks to the *rights and freedoms* of *natural persons* are assessed and managed. In Recital 75, examples of such risks are presented; Specifically, Recital 75 GDPR reads,

> 'The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
>
> where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
>
> where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership,
>
> and where the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
>
> where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order

to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or

where processing involves a large amount of personal data and affects a large number of data subjects.'

When performing a DPIA, the data controller, has to identify, assess and manage high risks to the *rights and freedoms of natural persons.* However, the focus of this Report is mainly on security risks, namely 'loss of confidentiality', 'loss of integrity', 'loss of availability', 'identification of the user / linkability'. The reason for that has already been explained in the Introduction section of this Report and has to do with the role of the Foundation as the developer of the IRMA app. This does not mean that other risks (apart from the classical security risks), will not be taken into consideration as the model of IRMA develops. The 'Risk Assessment' section of the Report will, thus, be continuously updated.

4.1 Unauthorised access to personal data (loss of confidentiality)

Confidentiality is defined as the *"property that information is not made available or disclosed to unauthorized individuals, entities, or processes"*[10]. In practice, all the measures implemented to ensure confidentiality are designed to prevent the information from being accessed by unauthorized individuals, entities or processes, while ensuring that the authorized individuals, entities or processes have access to it[11].

Threat[12] examples/scenarios

- An unauthorised actor gains access to the Foundation's database where the email address and the blinded PIN code of the IRMA user X are stored. He then combines it with the attributes that user X has disclosed to the Verifier and which are also processed by the Foundation. The unauthorised actor can then identify user X and can also track this user's behavior based on which services of which Verifiers the user has requested. *(see Measures 1,5,6)*
- An external attacker gains access to the user's personal data by monitoring the communication channel between the source of data and the Issuer. *(see Measure 2)*
- An external attacker gains access to the user's personal data by monitoring the communication channel between the Issuer and the IRMA app, until the attribute is sent to the app. *(see Measure 2)*
- The user's phone gets stolen and an unauthorised actor gains access to the user's IRMA app. *(see Measure 3)*

[10] ISO/IEC 27000:2016 Information technology -- Security techniques -- Information security management systems --
[11] ENISA, Guidelines for SMEs on the security of personal data processing, December 2016.
[12] A ***threat*** is any circumstance or event which has the potential to adversely affect the security of personal data, (n.5)

- While the IRMA user authenticates herself, another IRMA user who is behind her quickly scans the IRMA QR code of the original user.

Measures

1. **Access control** policy in the Foundation: Only one specific person has direct access to the database which contains the users' personal data
2. **Encryption in transit**: Communication channels (between "source of data" and the Issuer and between the Issuer and the app) are always encrypted using HTTPS/TLS. This encryption only applies in transit given that data do not appear in rest form (they are deleted as soon as possible). In cases where an Issuer has an external data source, the Foundation has agreements with this Issuer that such security measures are in place.
3. The user is required to provide her PIN code in order to proceed to any transaction via the MyIRMA app (receive attributes, disclose attributes etc.).
4. When the user decides to terminate IRMA on the MyIRMA webpage all data are immediately deleted. Thus, if the user wants to use IRMA in the future, she has to re-register from the start.
5. **Data minimisation**[13]:
    - The Foundation only processes the email address of the IRMA user (which is optional) as well as a blinded version of the PIN code for the purpose of registration of the user and for security reasons. The Foundation does not store information on which Verifier the user has revealed attributes to or from which Issuer the user has received attributes. When a user discloses attributes to a Verifier, then these attributes travel directly from the user's IRMA app to the Verifier, with the Foundation being involved only for the purpose of verifying the user's PIN during this transaction. At no point in such transactions does the Foundation learn to which verifier attributes are being disclosed.
    - The "source of data" provides user data to the Issuer through a protocol that ensures that only relevant information is disclosed (relevant being the minimum amount of data required to be able to perform the attribute issuance) .
    - With regard to the attribute(s) disclosed to the Verifier, only the attributes which are relevant and necessary for a transaction are disclosed. The disclosure of attributes that are contained in a credential is selective (eg. A credential may contain attributes such as: nationality, place of birth, date of birth, but any subset of these can be disclosed).
6. **Data retention**:

[13] This should be based on the 'need to know' principle, i.e. each role/user should only have the level of access to personal data that is strictly necessary for the performance of its relevant tasks. This is a central concept also in GDPR and is closely related to the principle of data minimization (art. 5(c) GDPR)

- Email address & blinded PIN code used for the user's registration are both stored in a special server which is located in the Netherlands and is called "MyIRMA"
- Decentralised architecture: attributes are stored only locally, on the user's phone, and not centrally in the computer systems of some "identity broker". This means that there is no one central place where attributes could be stolen from.

Vulnerabilities

- Data minimisation: It could be the case that a "source of data" does not limit itself only to the information that is needed for the attributes to be issued but rather provides more information to the Issuer than what is strictly relevant and necessary.
- Data minimisation: For the moment, there are no technical measures in place which enforce the Verifier to ask for a selective disclosure of attributes by the IRMA user. The Verifier is the one who decides which are the attributes that the user should disclose. The user gets to see this list of required attributes, and can then either accept or refuse. Technically, Verifiers have the option to ask for more attributes than the ones strictly necessary for the purpose of authenticating the user and providing the service.
- When the Issuer requests information from the source of data and when an attribute is issued by the Issuer to the user that requested it, this information constitutes in both cases personal data for a minimum period of time that is required for the information to be sent to the Issuer and for the attribute to be sent to the IRMA app.
- The user's PIN is not required in order to enter the IRMA app. It is required in cases where the user wants to proceed to transactions (request of attribute, disclosure of attribute). That means, that any non-user can gain access to the main screen listing the user's attributes of the IRMA app, whereby they can read the user's attribute (but not disclose them or receive new ones), and to the usage data of the user (the log history of the user, which if combined with the user's personal data – potentially from other sources- can lead to inferences about the user.)

Future steps

- The Foundation will add a new button to the IRMA app which will allow users to report, both to the Foundation as well as to the Dutch DPA ("Autoriteit Persoonsgegevens"), Verifiers who ask for more attributes than the ones strictly necessary for the purposes.

- The user's PIN will be required in order to access the IRMA app, and not only in order to proceed to transactions.

- The Foundation will require (in the form of an agreement) from every Issuer who wants to be part of IRMA, that they have appropriate technical measures in place to secure the communication channels both between the Issuer and the source of data, and between the Issuer and the IRMA user.

4.2 Unwanted modification/alteration of data (loss of integrity)

Integrity is defined as the property of "*accuracy and completeness*"[14]. In that sense, integrity implies maintaining the consistency, accuracy, and trustworthiness of information, over its entire life cycle. Data must not be changed in transit and measures must be undertaken to ensure that data cannot be altered by unauthorized individuals, entities or processes. From a practical point of view, this means that data cannot be modified in an unauthorized or undetected manner[15].

Threat examples/scenarios

- An external attacker gains access to the attributes sent to the user by monitoring the communication channel between the Issuer and the user. The attacker modifies the digital signature or the expiry date of the attribute in transit. The Verifier that will request the attribute in order to provide the service to the user will not be able to authenticate the user and therefore will not provide the service. (user will be denied a service) *(see Measure 4)*
- An external attacker gains access to the personal data requested by the Issuer, by monitoring the communication channel between the "source of data" and the Issuer. The attacker changes the personal data sent to the Issuer. Based on the (wrong) information that the Issuer receives, they issue wrong attributes to the user. The user is then provided services based on wrong attributes. *(see Measure 4)*
- The Issuer requests the "source of data" for relevant information about user X. However, the "source of data" incorrectly verifies the identity of X and instead provides to the Issuer information about user Ψ. *(see Measure 5)*

Measures

1. **Digital signature**: Attributes in IRMA carry a digital signature of the Issuer. Via this signature the Verifier can check the origin and the integrity of attributes. The digital signature is formed by a private key and a public key. This couple of keys is generated by the Issuer. The Issuer stores the private key, keeping it secret, and publishes the public key. The Verifier uses the public key to verify that the attributes that it received have been signed with the corresponding private key, which is known only to the Issuer, thus establishing that the origin and integrity of the attribute are guaranteed (this is called asymmetric signing)

[14] (n.4)
[15] (n.5)

2. **Expiration date:** Attributes have an expiry date, given by the Issuer, which can also be checked by the Verifier. If attributes have expired, they need to be refreshed by the user, by returning to the original Issuer.
3. **Encryption in transit**: Communication channels (between "source of data" and the Issuer and between the Issuer and the app) are always encrypted using HTTPS/TLS. This encryption only applies in transit given that data do not appear in rest form (they are deleted as soon as possible). In cases where an Issuer has an external data source, the Foundation has agreements with this Issuer that such security measures are in place.
4. The Foundation will require via a contract that all Issuers that receive information from external "sources of data", correct verification of users' identities.

4.3 Temporary or definitive unavailability of personal data (loss of availability)

Availability is defined as the property of *"information being accessible and usable when an authorized party demands it"*[16]. This means that the systems used to store and process information, as well as the information communication channels are all functioning correctly. In practice this is best ensured by uncompromised maintenance of the hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is software conflicts free[17].

Threat examples/scenarios

- IRMA's supporting assets are partially or completely damaged (ie. database of the Foundation) and all email addresses and blinded PIN codes are lost. IRMA users cannot use their attributes given that they cannot be authenticated with their PIN by the Foundation as IRMA app users.
- If the Foundation's system goes down, the whole IRMA system also goes down and users cannot use its services
- If the Foundation's servers go down and there is data loss, users will have to re-register to IRMA from scratch.

Vulnerabilities

- There are no back-ups for authentication of IRMA users. The user needs to re-register from scratch. This is an inconvenience for the user but it is a choice for reasons of security.
- The Foundation is a single point of failure (SPOF).

[16] (n.4)
[17] (n.5)

Future steps

- The Foundation is working on developing a backup /restore mechanism for the user's attribute wallet, including salt, such that IRMA's privacy and security guarantees are sustained. This mechanism will be such that if an earlier made backup from phone A is restored on phone B, then the attributes on phone A are made unusable.

- The Foundation is working on making it possible to run multiple copies of the central server[18] simultaneously, so that if one goes down other copies take over. As the Foundation's server is currently the only SPOF in the entire IRMA system, once this "future step" is taken, IRMA will have no SPOF anymore.

4.4 Identification of the user / Linkability[19]

In order to determine whether an individual is identifiable, all means that would allow the said individual to be identified and which are available to or accessible by the data controller or any other person must be taken into consideration. This includes information that is public, held or obtained otherwise, including over the Internet.

Threat examples/scenarios

- The Issuer of a non-identifying attribute tracks the behavior of the IRMA user with regard to this attribute (eg. to which Verifiers the user has disclosed the attribute, how often does the user disclose the attribute etc.) in order to build a profile of the IRMA user.
- IRMA user X receives a non-identifying attribute (eg. gender) from the Issuer. X is identified by the Issuer at the time of the issuance of the gender attribute. At a later point the Issuer colludes with one of the Verifiers (to whom X has disclosed the gender attribute) and both parties link their databases in order to identify X who used the Verifier's service.
- The same Verifier links non-identifying attributes that have been disclosed by one IRMA user over a period of time, in order to identify the user.
- IRMA user X receives an identifying attribute (eg. bank account number) from the Issuer. The Issuer, who knows that this bank account number belongs to user X, sees the Verifier's log entries (colludes with the Verifier), and thereby infers that it was user X who disclosed that attribute at that time.

---

[18] A central server is established so as to check the user's PIN (before a user receives or discloses attributes, we want to be sure that she entered her correct PIN, for reasons of security) and allows the IRMA session only to proceed if the PIN is correct. This means that this server must be able to prevent an IRMA session from proceeding if an incorrect PIN was entered.

[19] "Unlinkability relates to the ability of pieces of information to be related to each other and to an individual. Anonymity clearly falls within it.", EDPS Preliminary Opinion on privacy by design, Opinion 5/2018, p.13.

Measures

1. IRMA's purpose is privacy-friendly authentication and singing in the online environment based on attributes. Authentication is different from identification. If the IRMA user sends to a Verifier their ">18" attribute issued by their bank (Issuer), then the Verifier can tell that that attribute is authentic using the signature over the attributes. So the Verifier has authenticated the user's attribute, without identifying them. **Attributes can be non-identifying**. There are two categories of attributes: attributes that are uniquely identifying (eg. Bank account number is associated only with one person) and attributes that are not identifying (eg. Gender). Combinations of non-identifying attributes may together still identify a user.
2. **Multi-show unlinkability**: when an IRMA user discloses the same non-identifying attribute (e.g. her gender attribute) twice, then it is not possible for the Verifier to link these two transactions as coming from the same user. Put differently, this situation is indistinguishable for the Verifier from two distinct users both disclosing their own gender attributes (that happen to have the same value). This means that someone's attribute disclosures over time cannot be linked.

3. **Issuer unlinkability**: This means that an Issuer of attributes cannot trace the disclosures of these attributes by a user, not even when the issuer colludes (in any way) with a Verifier and both parties put their data together (they may try anything but will never succeed in breaking this property). Of course, this does not work for identifying attributes, like the bank account number, but it does work for non-identifying attributes, like the gender. Issuer unlinkability only comes into play when we assume that a nefarious Issuer colludes with Verifiers to link user disclosures.

Vulnerabilities

- There are identifying attributes which can lead to the identification of the IRMA user.)
- The decentralised architecture that is planned and will address the issue of availability, will raise issues for the identification of the users. Timing attacks might take place in cases where the key share server colludes with the Verifier.
- The expiry dates that are attached to the attributes (for reasons of integrity[20]) could lead to linkability issues.

Future steps

- The Foundation is considering to diminish the period of time that "log data" are retained.

[20] See above, Section 4.2, Expiry dates are one of the measures to ensure integrity.

- An enhanced version of the keyshare server is under development by the Foundation. The sophisticated cryptographic measures that will be ultimately put in place will make timing attacks impossible even of the keyshare server attempts to collude with any or all Verifiers.