SURYS

File verification functions of Photometrix SDK version 1.2.3

November 2020

CSPN Security Target

Version

Date	Version	Author	Comments
10/07/2019	1.0	L. GAUDIN	First version
23/10/2019	1.1	L. GAUDIN	Minor changes
04/11/2019	1.2	L. GAUDIN	Added traceability matrix and security needs for critical assets.
02/12/2019	1.3	L. GAUDIN	Minor changes. Consistency checks
02/03/2020	1.4	L. GAUDIN	ANSSI remarks taken into account
12/10/2020	1.5a	L. GAUDIN	Update linked with official feedback
09/11/2020	1.6	L. GAUDIN	Confidential remove Add element “App Security” in 5.2 Remove T.Application leak in 7.2 Add T.Application alteration tracability in 7.2
10/11/2020	1.7		Document restructuration following ANSSI remarks

References

Date	Version
[GUIDES]	*Photometrix Verifier Core – SDK for Android*, November 2020

Index

1 Product Identification

Editor	Surys
Editor Web site	Surys.com
Commercial name of the product	Photometrix Verifier Core
SDK version **Smartphone compatibility list**	1.2.3 Samsung galaxy S6 and above
Type of product	Android SDK

2 Glossary and terms

Authentication	Process to ensure the conformity of the **Photometrix™ code**.
Document holder	Person who gives this **Photometrix™** file to make authentication.
Photometrix™ Certificate	Public Key used in the authentication process
PhotoMetrix™ Code	2D printed representation of a **Photometrix™ file** that contains Authentication data and other customer specific data.
PhotoMetrix™ Application	Control application using the SDK **Photometrix™** installed on an Android or IPhone
Photometrix™ server	Server that contains **Photometrix™ Certificates** used in the authentication process.

3 Product description

3.1 General description of the product

Photometrix™ is an innovative 2D bar code that enables automated photo authentication without the need to connect to a centralized database. This security is based on the integration, in an encrypted 2D bar code, of the digital signature of the photograph.

This code can be printed on any media to then allow reading by a portable device (smartphone for example) or fixed (security gate). This code can also be present in dematerialized form in a Smartphone application. Thus the carrier presents his identity in digital form to the control system (smartphone of the controller or terminal of the security gantry)

Photometrix Digital ID

Thus, whatever the type of authentication request, the user can produce a paper document, an authentication card type document or a smartphone screen to authenticate.

Photometrix™ can be printed on any paper, PVC card or Polycarbonate card with 300DPI printing.

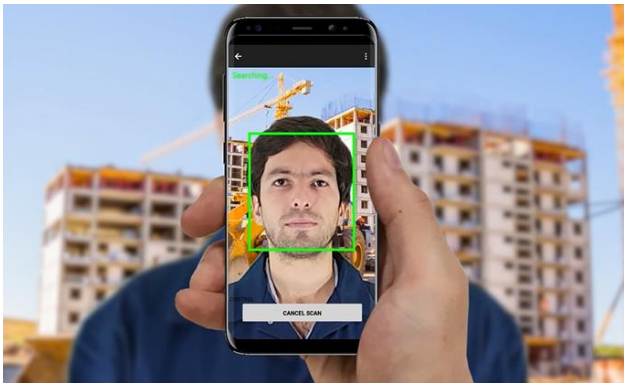
The generation of **Photometrix™** is immediate via a dedicated and centralized hardware and software module. This solution can therefore be used with decentralized personalization hardware for an immediate need (installation sites or temporary installations to be secured) or a centralized platform depending on the type of customization technology used or the security conditions for preparing these identification documents.

For example please see below an authentication scenario with a smartphone.

In order to control the authenticity of the ID document, the operator only needs a smartphone with a 2K camera. For Document holder control, two options, which can be implemented at the same time, can be used:

Photometrix Control

Facial recognition: The Photometrix™ code is scanned. Once the ID picture has been authenticated, it becomes a trusted element on which the facial recognition process will be based. This function is optional and is not included into the scope of the current document.



Face control

Fingerprint control using a fingerprint module connected to the smartphone.

Optional or can replace the facial recognition, fingerprint can be used to check Document holder.
Same basic procedure, document holder presents its fingerprint and control is immediate in an offline mode. This function is optional and is not included into the scope of the current document.

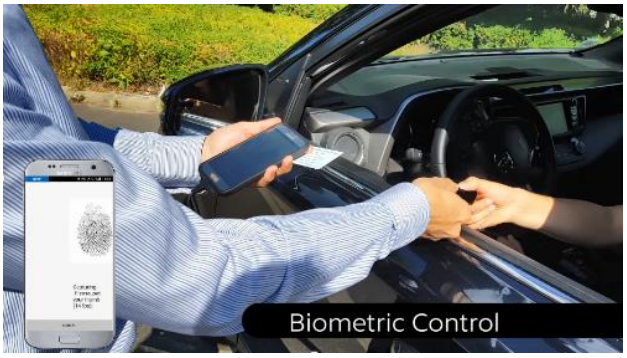


Figure 1 - Fingerprint control

SURYS proposes two technical approaches to provide final user tools to control **Photometrix™** Codes

- Control application developed by SURYS based on customer specifications
- SDK with SURYS support in order to let the customer capability to include **Photometrix™** control into its own application.

The purpose of this security target is to evaluate the SDK using a generic control application.

3.2 Product usage

3.2.1 Photometrix creation process

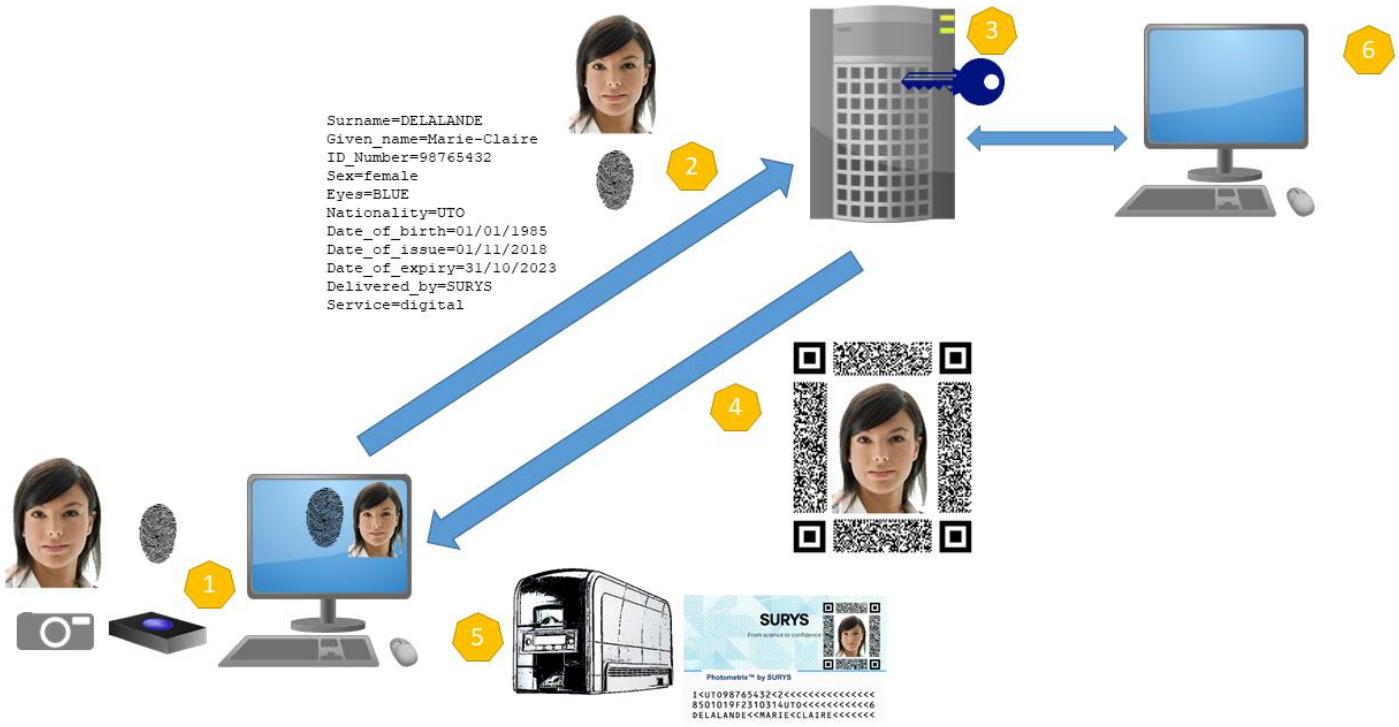
To authenticate the photograph and check its non-falsification, SURYS proposes an encoding mechanism, to note the immediate vicinity of the image on the document security features that will ensure easy verification using a smartphone or from any camera.

To do this, we defined a special encoding for representing stable character of photography, which will ensure that it has not been manipulated. From the digital photography of bearer, our system is extracting a number of features, by image processing. It will be chosen elements of biometrics. This data is then extracted using a likelihood priority that allows to keep only the most efficient for detecting manipulation of the document. They are then compressed to represent only a few bytes of information. Additional data or Metadata can be included in the payload.

These stable characters can then be associated with intrinsic data bearer document (for example, name, document number, date of birth,...), or metadata thereof (classification, data from external databases , conditions of use...), or possibly even a "payload" as a fingerprint represented in the form of a code of minutiae. The full payload is then signed by a cryptographic signature compact public key (eg ECDSA - Elliptic Curve DSA), to prove the information have been issued by a trusted source.

Photometrix Card Sample illustrated with Biometrics data included in the PhotoMetrix code

This data is represented as a visual two-dimensional code represented by pixels, the "**PhotoMetrix™ Code**" which included a number of redundant property to prevent reading difficulties. The **PhotoMetrix™ Code** is built in a series of landmarks, typically four to flat surfaces, which also included the image to secure. These landmarks allow the recovery by image processing for both the image and the code. This adjustment is to rebuild, despite a sometimes tricky angle, all the components of **PhotoMetrix™ Code** as they would found the original flat surface. The number of landmarks may be adapted according to the target surfaces (such as cylinders, cones, etc ...). The elements to straighten are included in to ensure optimal recovery. The entire **PhotoMetrix™ Code** can then be printed on the surface of the identity document or any other medium designed for this purpose.



Creation process

Step	Description
1	The citizen is enrolled. Photo and Fingerprint are captured through dedicated hardware. Additional data are typed by the operator on the computer.
2	Data are sent through a secure HTTPS channel via a web service to the Photometrix Server
3	Using a private key stored in a secured HSM, the server generates the Photometrix™ data
4	The Photometrix file in PNG, JPG or PDF format is sent back.
5	The Photometrix data is managed by customer software to manage full card personalization.
6	Administrative data are available from the Photometrix server to follow up Request Numbers, Key Management etc…

3.2.2 Photometrix verification process

Once the document is issued, it is necessary that it can be controlled easily and quickly. In a context that may be unstable and where rapid decision-making is necessary, the Smartphone Automated Authentication feature of the **Photometrix™** is a real benefit.

The code is constructed in such a way that it is automatically authenticated using a traditional smartphone and a secure application developed specifically for the end use.

Authentication is localized without the need to be connected to a central database or network of any kind.

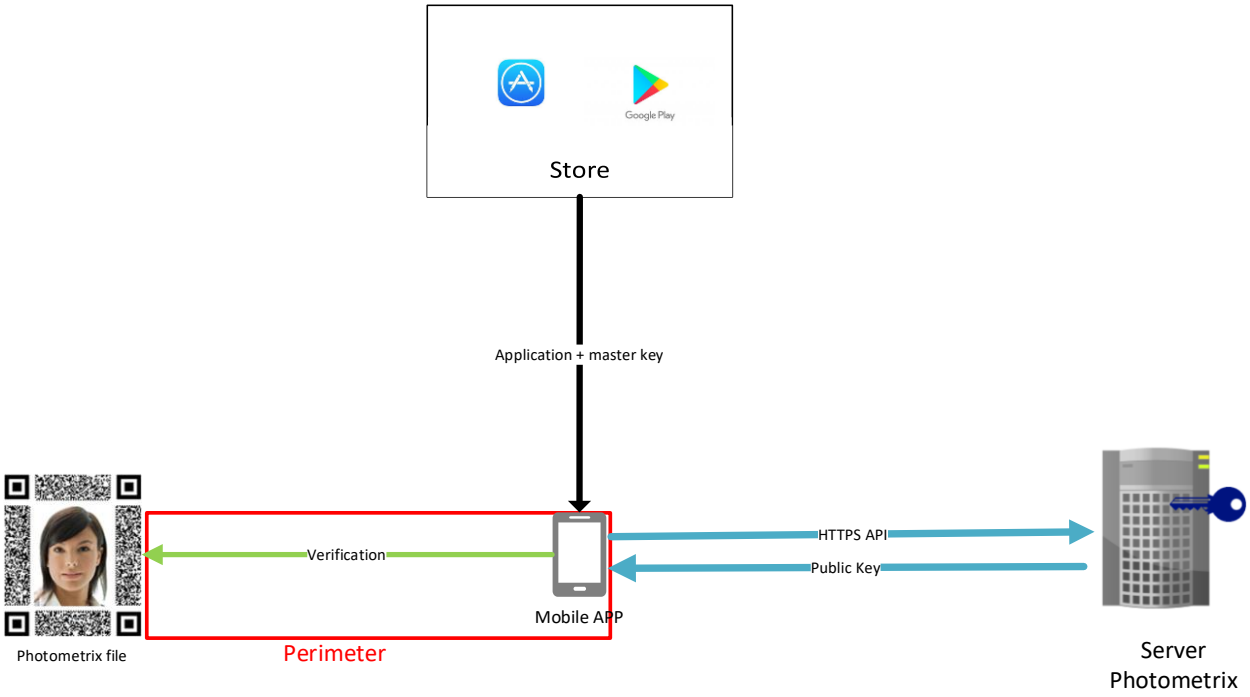
Photometrix Use

The **Photometrix™** application will decrypt the 2D code and compare certain elements of the photograph printed on the card, to the digital signature of the photo recorded during the issuance of the card to ensure that the photograph has not been manipulated. If the check is successful, some variable data will be extracted from the code so that the controller can also confirm that they have not been modified.

A facial check may also be used to verify that the person presenting the document with the **Photometrix™** component is the person named on this document. This technology can be implemented on smartphone or any other hardware and software solution.

4 Evaluation Perimeter

4.1 ToE perimeter



The ToE perimeter is defined as follow:

- A generic control application using the SDK **Photometrix™** installed on Android.

Photometrix™ server, corresponding communications, and Android Application store (including communication with them) are outside the ToE perimeter.

It should be noted that each **Photometrix™ application** download from app store is specific to one customer (e.g keys included in the application are specifically generated for one customer).

4.2 Limit of the evaluation

It should be noted that the evaluation is limited to the verification of the Photometrix file signature in order to prove its authenticity. The evaluation doesn't include Image processing that are implemented in the **Photometrix™** solution.

4.3 Operating environment

The environment that is needed to operate the ToE is composed of

- A generic mobile **PhotoMetrix™ application**
- A smartphone with Android 9.0
- A **PhotoMetrix™ server** (Nginx 1.10.3)
- The Android application store

5 Security Problem Definition

5.1 Users

The users that may interact with the ToE are the following:

User : person who will use Photometrix Verifier Core in order to develop his own application which will verify the **PhotoMetrix™** file.

5.2 Assumptions

User not evil

User are trained for performing the tasks they are responsible for. They follow instructions of the ToE and they are not hostile. They are supposed to follow instructions given in [GUIDES].

The user is supposed to connect every day to update **PhotoMetrix™ Certificates** including the revocation list.

Secure application

The application developed using the Photometrix Verifier Core is responsible not to harm or lower TOE's security. In particular, the application:

- shall not bypass Photometrix Verifier Core security and is supposed to be developed in a secure and responsible way;
- Shall guarantee master certificate's integrity and authenticity;
- Shall guarantee configuration file's integrity;
- Shall use the security functions provided by the SDK whenever these functionalities are necessary

The application is supposed to be installed on a phone up-to-date and free of malicious software.

Enrollment

The **PhotoMetrix™** creation process (see 3.2.1) is considered secured and is not included in the perimeter of the ToE.

Backend

The **PhotoMetrix™** backend (i.e the **PhotoMetrix™ server**) is considered secured and is not included in the perimeter of the ToE.

5.3 Critical assets

5.3.1 Sensitive data from the environment

A.PhotoMetrix™ certificate

A public key used to verify **PhotoMetrix™ file** associated with an interval validity date (after this date no **PhotoMetrix™ file** can be issued for this **PhotoMetrix™ Certificate**. Each public key is linked to a value page of **PhotoMetrix™ file** (i.e 100 000). Security needs for this asset are : integrity and authenticity.

5.3.2 Assets of the ToE

A.Photometrix_file

A **Photometrix™ file** contains a template and customer's data.

A template contains salient characteristics of the picture used in the verification process of the photo.

Customer's data are data formatted by the customer based on a configuration file. It includes the expiration date of the **PhotoMetrix™ file** and a serial number.

This file is signed by an asymmetric process (A.PhotoMetrix™ certificate). The signature result is included in the **PhotoMetrix™ file**. Security needs for this asset are: integrity and authenticity[1].

5.4 Threat model

5.4.1 Attackers

Attacks on the ToE are performed by a malicious person that want to usurp an identity when controlled by the user of the ToE. It could be the modification of the **PhotoMetrix™** file or the introduction of malicious data during the verification process performed by the ToE.

5.4.2 Threats

T.PhotoMetrix™ file alteration

The attacker manages to modify, temporary or permanently, the **PhotoMetrix™** file.

T.PhotoMetrix™ certificates alteration

[1] The Photometrix File contains Customers data and Template that need integrity. The whole file need also authenticity

The attacker attempt to alter or modify the **PhotoMetrix™ certificates** in order to modify **PhotoMetrix™ file** signature.

6 Security functions

SF.Verification function of public PhotoMetrix™ key

PhotoMetrix™ certificates are verified in integrity by the ToE. The ToE ensures that keys are neither present in the revocation list nor expired. Keys are also verified in authenticity using the Master Key stored in the application.

SF.Verification function of Photometrix file

The ToE checks the authenticity of the **PhotoMetrix™ file** by verifying the signature of **PhotoMetrix™ files**, signed by the **PhotoMetrix™ certificate** corresponding to the serial number of the **PhotoMetrix™ file**. **PhotoMetrix™ files** are signed using ECDSA Algorithm with ECDSA-SHA256 Keys. (Generation of the signature is outside the scope of evaluation)

7 Rationale

7.1 Assets/threats traceability

		T.PhotoMetrix™ file alteration	T.PhotoMetrix™ certificates alteration
Environmental asset	**A.PhotoMetrix™ certificate**		X
TOE asset	**A.Photometrix™ file**	X	

7.2 Threats/Security function traceability

	SF.Verification function of public PhotoMetrix™ key	SF.Verification function of Photometrix file
T.PhotoMetrix™ file alteration		X
T.PhotoMetrix™ certificates alteration	X	

SURYS

From science to confidence