

# Terms and conditions for the use of video identification and qualified electronic signature

## The service offered

Before opening a new business relationship, Banca dello Stato del Cantone Ticino (hereinafter, the "Bank") is obliged to check the identity of potential clients. To this end and in collaboration with Swisscom (Switzerland) SA (hereinafter, "Swisscom"), it offers clients the option of identifying themselves online by video (hereinafter, "Video Identification"). This means of identification is possible only for individuals aged 14 or more who are domiciled in Switzerland or notaries authorised to practise in Switzerland in accordance with Art. 36 VSB20.

By using the Video Identification and Qualified Electronic Signature service, the user acknowledges that he/she has read, understood and accepts these user terms and conditions. In particular, he/she is aware that Video Identification is a service provided by the Bank in collaboration with Swisscom and that the personal details he/she has provided to the Bank will be forwarded to Swisscom for incorporation into the proscribed video identification and qualified electronic signature procedures. The user thus authorises the Bank to transmit that data to Swisscom, releasing it from its duty of bank-client confidentiality (and from any other legal or contractual confidentiality requirements).

## How does Video Identification and Qualified Electronic Signature work?

Video identification is initiated by the user via the Bank's account opening site, with the user entering his own personal details, selecting the desired banking products and services and accepting these Terms of Use. The user is then connected to a website under the exclusive domain of Swisscom to initiate video identification with a Swisscom operator (in accordance with the procedure adopted by Swisscom). During the video identification, the Swisscom operator takes several photographs of the person to be identified, collect a copy of his/her identity document (passport or identity card listed in Table A of Annex 1), collect a copy of a his/her residence permit (B, C) where applicable, compares and checks the completeness and accuracy of the data previously provided by the user to the Bank with those of the identity document.

The identification process managed by Swisscom continues with the display of the basic banking documentation and that relating to the products and services chosen by the user. As a further check, a temporary authorisation code (TAN hereinafter) is sent to the user via SMS and entered into the Swisscom form before starting the qualified signature process.

The user is then asked about his actual intention to sign the documents, and in case of his affirmative reply, a second TAN is sent to them via SMS and entered into the Swisscom form as a qualified electronic signature. Once the video identification and qualified signature process has been completed, Swisscom sends the collected data (photographs, video recording and electronically signed documents) to the Bank. These data, collected by Swisscom solely for the purpose of being transmitted to the Bank, are permanently deleted by Swisscom within 10 days of completion of the video identification.

## Terms and conditions for proper Video Identification and Qualified Electronic Signature

All individuals aged 14 or more who are domiciled in Switzerland and have a valid passport or ID card according to table A (Annex 1) may access the Video Identification service. Moreover, for foreign nationals a valid copy of the residence permit is required (no surrogate or temporary certificate is accepted).

The user must have a device (computer, smartphone or tablet) with a video camera and microphone and a Windows (for computers), Android or iOS operating system.

The user accepts these user terms and conditions by expressly confirming acceptance at the start of the Video Identification procedure.

### **What level of security does Video Identification and Qualified Electronic Signature?**

The Bank and Swisscom observe the statutory provisions on data protection and use IT infrastructure managed in accordance with the technical provisions and usual practices in the banking sector. Internet data are always transmitted via a secure connection.

On the other hand, there are risks entailed in using all normal means of electronic communication (e-mails and text messages) and in particular in the transmission of data via an open network. Such data may be intercepted and saved by third parties (inside and outside Switzerland), regardless of whether the sender and the recipient are on the Swiss territory.

The user should therefore be aware of the fact that a third party may be able to access his/her data sent by the usual means of electronic communication and also that encrypted communication between the issuer of the data and the recipient does not exclude the possibility of a third party identifying the nature of the contractual relationship between the user and the Bank.

Consequently, the user is generally advised to use up-to-date system and security software (for example by installing firewalls and anti-malware programs).

### **Data protection**

We confirm that your personal data will be processed by us in accordance with the Swiss Federal Act on Data Protection and more specifically in accordance with the Privacy Policy published on our website [www.bancastato.ch](http://www.bancastato.ch). The Privacy Policy may be obtained in paper form upon your request.

## Annex 1

Table A - Nationalities and permitted ID documents

Country	Passport	Acceptance of ID document conditioned by (a) clause	ID card	Document not Valid for qualified electronic signature
Australia	Accepted	*	Not Accepted	
Austria	Accepted		Accepted	
Belgium	Accepted		Accepted	
Bosnia & Herzegovina	Accepted		Accepted	*
Bulgaria	Accepted		Not Accepted	
Canada	Accepted	*	Not Accepted	
Cape Verde	Accepted	*	Not Accepted	
Chile	Accepted	*	Accepted	*
Croatia	Accepted		Not Accepted	
Czech Republic	Accepted		Accepted	
Denmark	Accepted		Not Accepted	
Dubai/VA Emirate	Accepted	*	Accepted	*
Egypt	Accepted	*	Not Accepted	
Estonia	Accepted		Accepted	
Faroe Islands	Accepted		Not Accepted	
Finland	Accepted		Accepted	
France	Accepted		Accepted	
Georgia	Accepted	*	Accepted	*
Germany	Accepted		Accepted	
Ghana	Accepted	*	Not Accepted	
Greece	Accepted		Not Accepted	
Greenland	Accepted		Not Accepted	
Hungary	Accepted		Accepted	
Iceland	Accepted		Not Accepted	
India	Accepted	*	Not Accepted	
Indonesia	Accepted	*	Not Accepted	
Iran	Accepted	*	Not Accepted	
Ireland	Accepted		Not Accepted	
Israel	Accepted	*	Not Accepted	
Italy	Accepted		Not Accepted	
Kosovo	Accepted	*	Not Accepted	
Kuwait	Accepted	*	Not Accepted	
Latvia	Accepted		Accepted	
Lebanon	Accepted	*	Not Accepted	
Liechtenstein	Accepted		Accepted	
Lithuania	Accepted		Accepted	
Luxembourg	Accepted		Not Accepted	
Malaysia	Accepted	*	Not Accepted	
Malta	Accepted		Accepted	
Morocco	Accepted	*	Not Accepted	
Netherlands	Accepted		Accepted	
New Zealand	Accepted	*	Not Accepted	
Norway	Accepted		Not Accepted	
Pakistan	Accepted	*	Accepted	*
Poland	Accepted		Accepted	
Portugal	Accepted		Not Accepted	
Republic of China	Accepted	*	Not Accepted	
Republic of Cyprus	Accepted		Accepted	

Country	Passport	Acceptance of ID document conditioned by (a) clause	ID card	Document not Valid for qualified electronic signature
Republic of Macedonia	Accepted	*	Not Accepted	
Republic of Moldova	Accepted	*	Not Accepted	
Romania	Accepted		Not Accepted	
Russia	Accepted	*	Not Accepted	
Serbia	Accepted	*	Not Accepted	
Singapore	Accepted	*	Not Accepted	
Slovakia	Accepted		Accepted	
Slovenia	Accepted		Accepted	
South Africa	Accepted	*	Accepted	*
Spain	Accepted		Accepted	
Sweden	Accepted		Accepted	
Switzerland	Accepted		Accepted	
Taiwan	Accepted	*	Not Accepted	
Turkey	Accepted	*	Not Accepted	
United Kingdom	Accepted		Not Accepted	
United States	Accepted	*	Not Accepted	
Uruguay	Accepted	*	Not Accepted	
Vietnam	Accepted	*	Not Accepted	

A) In order to be accepted as part of the qualified electronic signature, the document must meet all of the following criteria:

- it must be valid for at least 3 months after the end of the identification process
- it was issued less than 10 years before the start of the identification process.

In any case, the date of issuance of the document is relevant for the determination of its validity, irrespective of possible validity extensions implemented by the governments of issuing countries.