



VoiceProof® Online – FAQ.

VoiceProof® Online is a software solution for online transaction verification. It includes on-line authentication of transaction signer and transaction content integrity validation.

1. What are available options for this product delivery?
VoiceProof® Online is available as SaaS (Software-as-a-Service) for small customers (100<#users<10,000) and “on-premises” for large customers (#users>10,000).
2. What kind of integration is required from small customer in SaaS model?
The customer is required to install a script on its web page and install thin client on one of its workstations. He should also deliver a list of its users to SentryCom.
3. What kind of software should user install?
The user should download and install thin client from SentryCom production web site.
4. How can you trust this web site?
SentryCom production web site carries digital certificate verifying its authenticity in accordance with industry standards.
5. How can you trust this downloaded thin client?
SentryCom thin client from production web site is digitally signed verifying its authenticity in accordance with industry standards.
6. How users enlist into this SaaS?
Customer-supplied users list contains user’s email. PC registration email will be sent with the one-time registration token, that cannot be re-used,
7. How can you trust this email?
This email is digitally signed and time-stamped by SentryCom.
8. What this email contains?
One-time registration link and signed instruction manual.
9. What exactly user registers?
User registers his PC and his Biometrics VoicePrint?
10. What Operating Systems and Browsers you support?
Microsoft - Win 2000, Win XP, Win Vista - with Internet Explorer.
11. What kind of microphone do you need?
Any kind – as long as you follow our instructions.
12. What are your microphone instructions?
Position microphone within 3-5 cm from the corner of your mouth .



13. I use my built-in mike in my laptop at ~20 cm distance for Skype. What's wrong with that?
Skype is telephony application. There is nothing wrong with the way you using your mike for Skype. In our application you need to get much closer to prevent acoustic echo from influencing your Biometrics VoicePrint.
- 14 . I am not comfortable with getting that close to my built-in mike. What do you suggest?
Use headset mike. It is the best option in terms of performance.
- 15 Should I test my mike first?
You bet . Go to **Control Panel/Sounds and Audio Device/Audio/Sound Recording** and setup recording control of microphone volume at about mid-scale .

Then go to **All Programs/Accessories/Entertainment/Sound Recorder**- start recording you own voice If you see response and hear playback - then you are OK If not - check your hardware.
- 15a. What if the room is too noisy?
What counts is not noise by itself, but speech to noise ratio.
If during the registration you receive the message:" We can't hear you "
- speak louder and if noise level (before you speak) is above 2 marks of the sound scale - you should reduce soundcard microphone volume recording control and speak louder.
16. How long registration takes?
Less then a minute.
17. Is it complicated?
We tell you to say few random digits – you say it – and that's it. Nothing fancy.
18. In what language?
In English. Our prompts are both seen on screen and heard in your speakers- very convenient.
19. Should I answer in English or my native language?
You should answer in English as well.
20. What will happen after successful registration?
You will receive 4-digit PIN by email.
21. You said that you register my PC ? What if I want to use your product from additional PC?
You can . You need to install thin client on that PC and re-register.
22. Should I call help-desk to re-register?
No. We enable re-registration if you are authenticated online. Use self-service – no need to bother with "Mother Maiden Name".



23. What will happen if somebody tape-recorded my voice and uses it for attack?
Our system will reject it.
24. What will happen if human impersonator is used for attack ?
Our system will reject it.
25. Are you saying that my voice is unique?
No. Your voice is not unique. But the chance that somebody has access to your PC , knows your 4-digit PIN and his voice is similar to yours is close to zero.
- 26 What will happen if I get cold?
As long as you can speak clearly – you can use the system.
- 26a Does the accuracy depends on intonation or pace?
No.
26. My microphone is broken. What should I do?
Replace it and re-register using self-service administration.
27. How I can trust that my VoicePrint is not stolen from your database?
Our database is password-protected and encrypted.
30. But people say this not enough. Can you elaborate?
Databases today are routinely password-protected and data-encrypted. But this is not regarded sufficient due to the nature of biometrics information. Therefore one must deal with the NATURE of biometrics information. First the database of biometrics information must be anonymous, namely biometrics data is not bound to any publicly know information such as person's name or ID number. For example: if biometric information is bound to the token such as email rtgy2374@bank.com , and bank stores independently the name of that email owner – then stealing that biometric information will do no good to the fraudster. If nevertheless – the biometric database is stolen – how do you store it? Biometric information must be stored in the binary irreversible form. Namely it must never store the data in the form of originally acquired image or audio.
On top of it there should be a way to revoke compromised binary data in case it is stolen. Text-dependent Voice Biometrics provides the way to do just that. One can change the vocabulary used by text-dependent Voice Biometrics to generate new VoicePrint and revoke the old one.
So what we achieve is anonymous, irreversible and replaceable central biometrics database.
- 31 Can you use you product for other things then signing online transactions?
You can use it for secure email (for-your-eyes-only) between the users, digitally signing any content, encrypting documents, etc.
32. Do you need to register to use all these functionalities?
Functionality that requires user authentication - needs registration. For example digital signing and opening encrypted documents.
Functionality that do not require user authentication – do not need registration. For example viewing signed documents and sending encrypted messages.



33. We are not comfortable with using Voice Biometrics. Can we use this product without it?
This opportunity exists for all customers (large or small), since our authentication scheme is scalable on demand. Instead of 3-factor authentication including Voice Biometrics – they may use 2-factor authentication. This is their money after all...
34. The users sometimes do not read manuals and do things they are not supposed to do. How you deal with that?
We provide software-only solution for cooperative users eager to protect their money and sensitive information. We do not provide “bad-user-proof” software.
35. But can you rely on user with security application?
Today it estimated that ~3% of the users fall victim to phishing – social engineering scheme to steal their passwords. In other words ~97% of the users follow instructions how to avoid phishing. Our goal is to provide this overwhelming majority with necessary protection.
36. The users will follow instructions – all right, but fraudsters will certainly do whatever they like to break-in. How you deal with that?
Whatever fraudster does -the system is designed to provide the highest security possible, at the same time being the most convenient for the users, and cost-effective for the customers (large or small). This is what we deliver.

For addition info:

<http://www.sentry-com.net/contactus.html>