1:1 Authentication

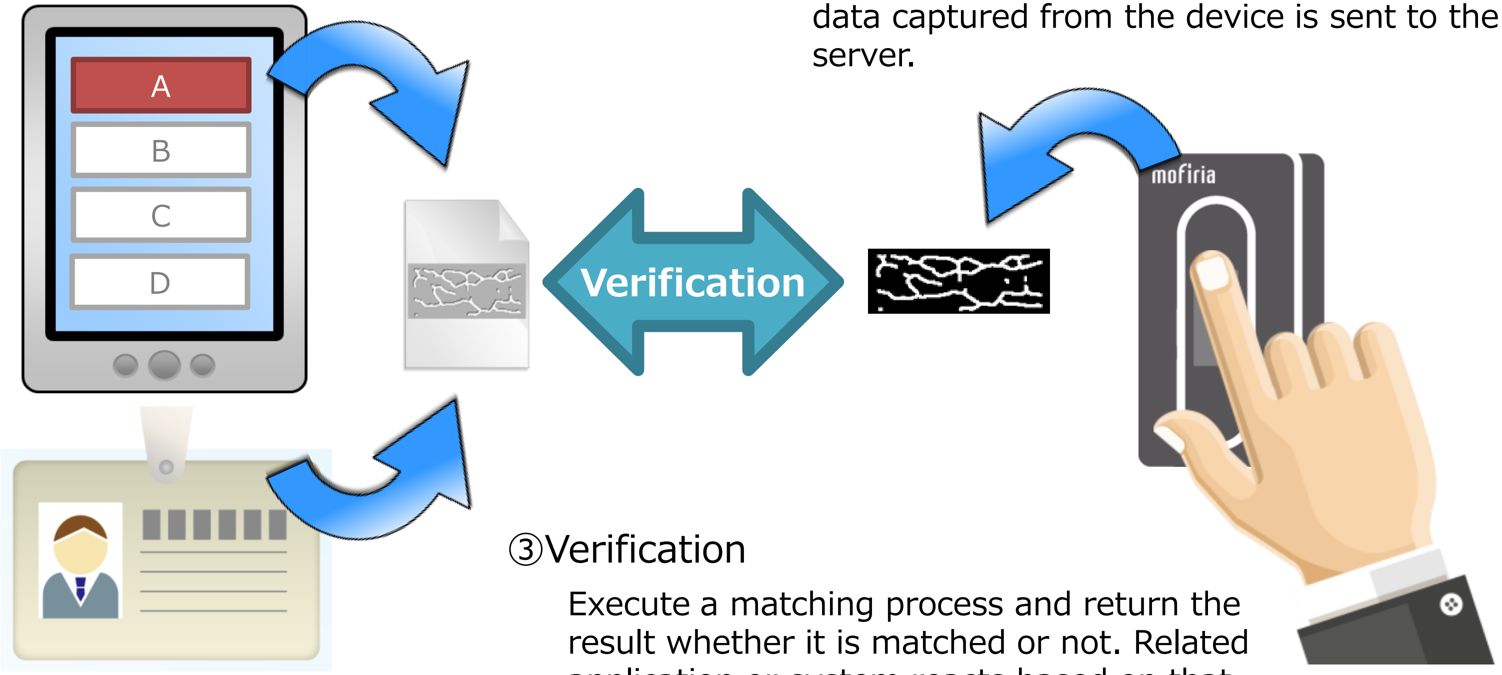
1:1 authentication (verification) is a method that calls a template for the person to be verified and then compare it with an actual finger vein pattern. It has lower usability compared with 1:N authentication (identification) but much higher accuracy and security.

①Specify a template to be verified

Specify a template to be verified by choosing a name, entering ID number, loading from an IC card or so.

②Load

For authentication in device, load the template specified at Step 1 into an authentication device.
For authentication on server, encrypted image data captured from the device is sent to the server.



③Verification

Execute a matching process and return the result whether it is matched or not. Related application or system reacts based on that result.

1:N Authentication

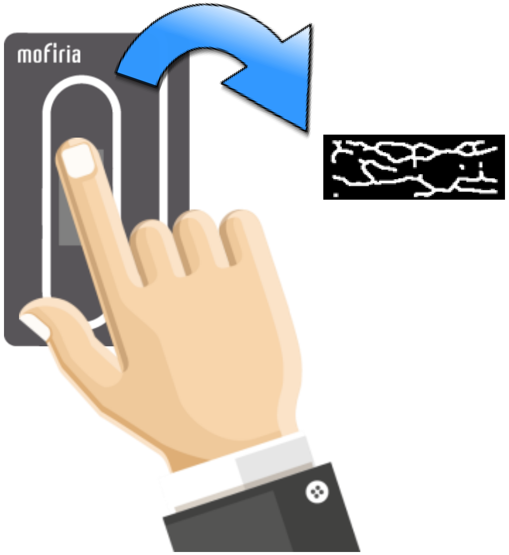
1:N authentication (identification) is a method that chooses the most suitable one from many pre-registered templates just by placing a finger on the device. Lower accuracy and speed than 1:1 authentication but better usability as all you need to do is to place a finger.

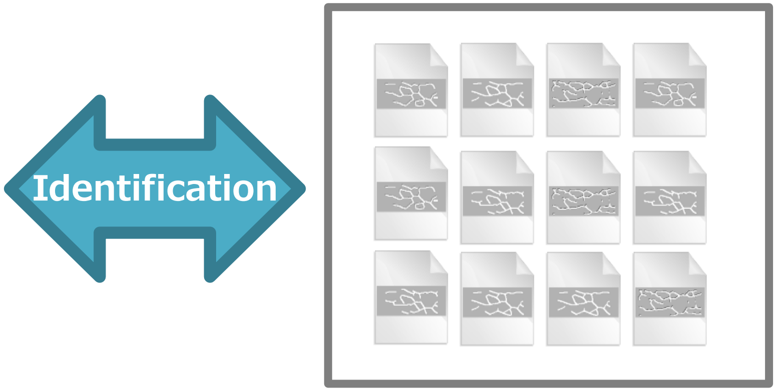
①Capture finger vein image

Capture finger vein image from device and encrypted data is sent to the server.

②Identification on server

Sent data is compared with pre-registered all templates on server. The more templates you have, the longer the process time would take.





③Return the result

If a corresponding template is found, it returns the related ID number.

｢The person who is placing a finger now is Mr.A ｣

Comparison of 1:1 and 1:N

	1:1	1:N
Usability	△	◎ ➔No need to input or specify other info.
Security	◎	△ ➔The more templates to be compared, the less accuracy it has in principle. ➔It needs some additional processes in case multiple candidates are found.
Processing speed	◎	△ ➔The processing time is basically longer since it compares with all templates.
Memory consumption	◎	△ ➔All templates need to be loaded on the main memory.